

PCT/JPG00/05482

16.08.00

日 本 国 特 許 庁

PATENT OFFICE
JAPANESE GOVERNMENT

REC'D 04 SEP 2000

WIPC PC

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日

Date of Application:

1999年 8月20日

09/80770

出 願 番 号

Application Number:

平成11年特許願第234368号

出 願 人

Applicant(s):

ソニー株式会社

PRIORITY
DOCUMENT

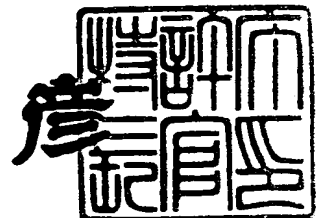
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)

CERTIFIED COPY OF
PRIORITY DOCUMENT

2000年 6月29日

特許庁長官
Commissioner,
Patent Office

近 藤 隆 彦



出証番号 出証特2000-3049976

【書類名】 特許願

【整理番号】 9900283403

【提出日】 平成11年 8月20日

【あて先】 特許庁長官 殿

【国際特許分類】 G11B 7/00

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

【氏名】 浅野 智之

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

【氏名】 大澤 義知

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

【氏名】 加藤 元樹

【特許出願人】

【識別番号】 000002185

【氏名又は名称】 ソニー株式会社

【代表者】 出井 伸之

【代理人】

【識別番号】 100067736

【弁理士】

【氏名又は名称】 小池 晃

【選任した代理人】

【識別番号】 100086335

【弁理士】

【氏名又は名称】 田村 榮一

【選任した代理人】

【識別番号】 100096677

【弁理士】

【氏名又は名称】 伊賀 誠司

【手数料の表示】

【予納台帳番号】 019530

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9707387

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 情報記録／再生システム、情報記録装置及び情報再生装置

【特許請求の範囲】

【請求項 1】 暗号化コンテンツ情報を暗号化されたまま記録媒体に記録するコンテンツ情報記録手段と、

上記暗号化コンテンツ情報からコンテンツ情報を暗号鍵により復号するコンテンツ情報復号手段と、

上記暗号鍵を暗号化する暗号鍵暗号化手段と、

上記暗号鍵暗号化手段により暗号化された暗号化暗号鍵を上記記録媒体に記録する暗号鍵記録手段と、

上記コンテンツ情報復号手段により復号されたコンテンツ情報を用いて上記記録媒体に記録された暗号化コンテンツ情報を再生する際に必要となる管理情報を生成する管理情報生成手段と、

上記管理情報生成手段により生成された管理情報を上記記録媒体に記録する記録手段とを備える情報記録装置と、

上記情報記録装置により暗号化コンテンツ情報と暗号化暗号鍵と管理情報が記録された記録媒体から上記管理情報を読み出す管理情報読出手段と、

上記記録媒体から上記暗号化暗号鍵を読み出す暗号鍵読出手段と、

上記記録媒体から上記暗号化コンテンツ情報を読み出すコンテンツ情報読出手段と、

上記管理情報読出手段により読み出された管理情報に基づいて上記記録媒体から暗号化暗号鍵と暗号化コンテンツ情報を読み出す位置を制御する読出位置制御手段と、

上記暗号鍵読出手段により読み出された暗号化暗号鍵から暗号鍵を復号する暗号鍵復号手段とを備える情報再生装置と

からなることを特徴とする情報記録／再生システム。

【請求項 2】 上記情報記録装置は、通信手段を用いて他の装置から伝送されてきた暗号化コンテンツ情報と該コンテンツ情報を暗号化するのに用いられた暗号鍵を受信する受信手段を備え、上記受信手段により受信した暗号鍵を上記暗号

鍵暗号化手段で暗号化するとともに、上記受信手段により受信した暗号鍵を用いて上記受信手段により受信した暗号化コンテンツ情報からコンテンツ情報を上記コンテンツ情報復号手段により復号して、上記管理情報生成手段により管理情報を生成することを特徴とする請求項 1 記載の情報記録／再生システム。

【請求項 3】 上記暗号化コンテンツ情報は、映像情報であることを特徴とする請求項 1 記載の情報記録／再生システム。

【請求項 4】 上記暗号化コンテンツ情報は、音楽情報であることを特徴とする請求項 1 記載の情報記録／再生システム。

【請求項 5】 暗号化コンテンツ情報を暗号化されたまま記録媒体に記録するコンテンツ情報記録手段と、

上記暗号化コンテンツ情報を復号するコンテンツ情報復号手段と、

上記コンテンツ情報復号手段により暗号化コンテンツ情報から復号されたコンテンツ情報を用いて上記記録媒体に記録された暗号化コンテンツ情報を再生する際に必要となる管理情報を生成する管理情報生成手段と、

上記管理情報生成手段により生成された管理情報を上記記録媒体に記録する記録手段と

を備えることを特徴とする情報記録装置。

【請求項 6】 通信手段を用いて他の装置から伝送されてきた暗号化コンテンツ情報と該コンテンツ情報を暗号化するのに用いられた暗号鍵を受信する受信手段と、

上記受信手段により受信した暗号鍵を暗号化する暗号鍵暗号化手段と、

上記暗号鍵暗号化手段により暗号化された暗号化暗号鍵を上記記録媒体に記録する暗号化暗号鍵記録手段と

をさらに備え、

上記コンテンツ情報復号手段は、上記受信手段により受信した暗号鍵を用いて、上記受信手段により受信した暗号化コンテンツ情報からコンテンツ情報を復号することを特徴とする請求項 5 記載の情報記録装置。

【請求項 7】 記録媒体から記録媒体識別情報を読み出す記録媒体識別情報読出手段と、

上記記録媒体識別情報読出手段により読み出された記録媒体識別情報を用いて
上記暗号鍵暗号化手段により上記暗号鍵を暗号化するために用いる第 1 の暗号鍵
を決定する第 1 の暗号鍵生成手段と

をさらに備えることを特徴とする請求項 6 記載の情報記録装置。

【請求項 8】 上記暗号鍵暗号化手段により上記暗号鍵を暗号化するために用
いる第 1 の暗号鍵を決定する第 1 の暗号鍵生成手段と、

上記記録媒体から記録媒体識別情報を読み出す記録媒体識別情報読出手段と、

上記記録媒体識別情報読出手段により読み出された記録媒体識別情報を用いて
上記第 1 の暗号鍵を暗号化するために用いる第 2 の暗号鍵を決定する第 2 の暗号
鍵生成手段と

をさらに備えることを特徴とする請求項 6 記載の情報記録装置。

【請求項 9】 記録媒体から記録媒体識別情報を読み出す記録媒体識別情報読
出手段と、

上記記録媒体に暗号化して格納されている第 1 の暗号鍵を読み出す暗号鍵読出
手段と、

上記暗号鍵読出手段により読み出される暗号化された第 1 の暗号鍵を復号する
ための第 2 の暗号鍵を上記記録媒体識別情報読出手段により読み出された記録媒
体識別情報に基づいて決定する第 2 の暗号鍵生成手段と、

上記第 2 の暗号鍵生成手段で生成された第 2 の暗号鍵を用いて暗号化された第
1 の暗号鍵を復号する第 1 の暗号鍵復号手段と

をさらに備え、

上記暗号鍵暗号化手段は、上記受信手段により受信した暗号鍵を上記第 1 の暗
号鍵復号手段により復号された第 1 の暗号鍵を用いて暗号化することを特徴とす
る請求項 6 記載の情報記録装置。

【請求項 10】 暗号化コンテンツ情報と該暗号化コンテンツ情報からコンテ
ンツ情報を復号するための暗号鍵を暗号化した暗号化暗号鍵と管理情報が記録さ
れた記録媒体から上記管理情報を読み出す管理情報読出手段と、

上記記録媒体から上記暗号化暗号鍵を読み出す暗号鍵読出手段と、

上記記録媒体から上記暗号化コンテンツ情報を読み出すコンテンツ情報読出手

段と、

上記管理情報読出手段により読み出された管理情報に基づいて上記記録媒体から暗号化暗号鍵と暗号化コンテンツ情報を読み出す位置を制御する読出位置制御手段と、

上記暗号鍵読出手段により読み出された暗号化暗号鍵から暗号鍵を第 1 の暗号鍵により復号する暗号鍵復号手段とを備える

ことを特徴する情報再生装置。

【請求項 1 1】 記録媒体から記録媒体識別情報を読み出す記録媒体識別情報読出手段と、

上記記録媒体識別情報読出手段により読み出された記録媒体識別情報を用いて上記暗号鍵復号手段により上記暗号鍵を復号するために用いる第 1 の暗号鍵を決定する第 1 の鍵生成手段とをさらに備える

ことを特徴とする請求項 1 0 記載の情報再生装置。

【請求項 1 2】 上記暗号鍵復号手段により上記暗号鍵を復号するために用いる第 1 の暗号鍵を決定する第 1 の鍵生成手段と、

上記記録媒体から記録媒体識別情報を読み出す記録媒体識別情報読出手段と、

上記記録媒体識別情報読出手段により読み出された記録媒体識別情報を用いて上記第 1 の暗号鍵を暗号化するために用いる第 2 の暗号鍵を決定する第 2 の鍵生成手段とをさらに備える

ことを特徴とする請求項 1 0 記載の情報再生装置。

【請求項 1 3】 記録媒体から記録媒体識別情報を読み出す記録媒体識別情報読出手段と、

上記記録媒体に暗号化して格納されている第 1 の暗号鍵を読み出す暗号鍵読出手段と、

上記暗号鍵読出手段により読み出される暗号化された第 1 の暗号鍵を復号するための第 2 の暗号鍵を上記記録媒体識別情報読出手段により読み出された記録媒体識別情報に基づいて決定する第 2 の鍵生成手段と、

上記第 2 の鍵生成手段で生成された第 2 の暗号鍵を用いて暗号化された第 1 の暗号鍵を復号する第 1 の暗号鍵復号手段とをさらに備える

ことを特徴とする請求項 1 0 記載の情報再生装置。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、安全にデータを授受することを可能にした情報記録／再生システム、情報記録装置及び情報再生装置に関する。

【0 0 0 2】

【従来の技術】

近年、情報をデジタル的に記録する記録機器及び記録媒体が普及しつつある。これらの記録機器及び記録媒体は、例えば、映像や音楽のデータを劣化することなく記録し、再生するので、データの質を維持しながら何度もデータをコピーすることができる。しかしながら、映像や音楽のデータの著作権者にしてみれば、自らが著作権を有するデータが、その質を維持しながら何度も不正にコピーされ、市場に流通してしまう恐れがある。このため、記録機器及び記録媒体の側で、著作権を有するデータが不正にコピーされるのを防ぐ必要がある。

【0 0 0 3】

このような著作権保護のためのシステムとして、例えば、ミニディスク（MD）（商標）システムにおいては、SCMS (Serial Copy Management System) と呼ばれる方法が用いられている。これは、デジタルインタフェースによって、音楽データとともに伝送される情報のことである。この情報は、音楽データが、copy free、copy once allowed、又はcopy prohibitedのうちのいずれのデータであるのかを表す。ミニディスクレコーダは、デジタルインタフェースから音楽データを受信した場合、SCMSを検出し、これが、copy prohibitedであれば、音楽データをミニディスクに記録せず、copy once allowedであれば、これをcopy prohibitedに変更し、受信した音楽データとともに記録し、copy freeであれば、これをそのまま、受信した音楽データとともに記録する。

【0 0 0 4】

このようにして、ミニディスクシステムにおいては、SCMSを用いて、著作権を有するデータが不正にコピーされるのを防いでいる。

【 0 0 0 5 】

また、著作権を有するデータが不正にコピーされるのを防ぐ別の例としては、Digital Versatile Disk(DVD)（商標）システムにおける、コンテンツスクランブルシステムがあげられる。このシステムでは、ディスク上の、著作権を有するデータが全て暗号化され、ライセンスを受けた記録機器だけが暗号鍵を与えられ、これにより暗号化されたデータを復号し、意味のあるデータを得ることができるようになされている。そして、記録機器は、ライセンスを受ける際に、不正コピーを行わない等の動作規定に従うように設計される。このようにして、DVDシステムにおいては、著作権を有するデータが不正にコピーされるのを防いでいる。

【 0 0 0 6 】

【発明が解決しようとする課題】

しかしながら、上記のミニディスクシステムが採用している方式では、SCMSがcopy once allowedであれば、これをcopy prohibitedに変更し、受信したデータとともに記録するなどの動作規定に従わない記録機器が、不正に製造されてしまう。

【 0 0 0 7 】

また、上記のDVDシステムが採用している方式は、ROMメディアに対しては有効であるが、ユーザがデータを記録可能なRAMメディアにおいては有効ではない。RAMメディアにおいては、不正者は、暗号を解読できない場合であっても、ディスク上のデータを全部、新しいディスクに不正にコピーすることによって、ライセンスを受けた正当な記録機器で動作するディスクを新たに作ることができるからである。

【 0 0 0 8 】

そこで、本件出願人が先に出願した特願平 1 0 - 2 5 3 1 0 号の特許出願においては、個々の記録媒体を識別するための情報（以下、媒体識別情報とよぶ）を記録媒体に持たせ、この情報はライセンスを受けた機器しかアクセスできないようにしている。すなわち、記録媒体上のデータは媒体識別情報と、ライセンスを受けることによって得られる秘密に基づく鍵によって暗号化し、ライセンスを受

けていない機器はデータを読み出しても意味のないものとしている。さらに機器にライセンスを与える際にはその動作を規定し、不正コピーを行わないようにする。ライセンスを得ていない機器は媒体識別情報にアクセスできず、また媒体識別情報は個々の媒体ごとに個別の値になっているため、ライセンスを受けていない機器がアクセス可能なすべての情報を新たな媒体にコピーしたとしても、そのようにして作られた媒体は、ライセンスを受けていない機器でもライセンスを受けた機器でも正しく情報が読み出せないようにしている。

【0009】

ところで、上記特許出願に係る記録機器では、他の機器とデータの送受信を行える例えば IEEE 1394 などのインタフェースを備えており、他の機器から伝送されたコンテンツデータを記録媒体に記録する場合が考えられる。

【0010】

この場合、コンテンツデータは、インタフェース上を、例えば、ソニー、松下、日立、東芝、インテルの5社によって開発された、Digital Transmission Content Protection 規格（この規格そのものはライセンスを受けないと見ることができないが、その概要を記した White Paper を、ライセンス組織である Digital Transmission Licensing Administrator (DTLA) のウェブページである <http://www.dtcp.com> から誰でも取得することが可能である）を用いて暗号化されて伝送されることが考えられる。この際、コンテンツデータはコンテンツキー Kc を用いて暗号化されて伝送され、さらにコンテンツキー Kc 自身も暗号化されるなど、安全な方法で上記記録機器に伝送される。

【0011】

記録機器が伝送されたコンテンツデータを安全に、すなわち不正コピーを許さないように、記録媒体に記録する最も簡単な方法は、暗号化されて伝送されたコンテンツデータをそのまま記録媒体に記録し、さらにこのデータの暗号化に使用されたコンテンツキーをこの記録システムにおいて用いられる方法で暗号化して媒体に記録することである。

【0012】

このようにすれば、記録機器は記録時に、大容量のコンテンツデータの処理が

ただ受信して記録するだけでよくなり、簡便に行える。

【0013】

しかしながら、上記の方式においては、コンテンツデータは暗号化されたまま記録機器に伝送されて媒体に記録されているため、再生時に不便である。

【0014】

すなわち、本来であれば、AVコンテンツを再生する際には、特に、早送り又は巻き戻ししながらの再生など、いわゆるトリックプレイを行うためには、コンテンツデータのフォーマットと構造を認識して、それに対応して記録媒体のどのデータを読み出すかを決定するなどの制御を行う必要がある。

【0015】

ところが、上記の方式においては、記録媒体からコンテンツデータを読み出して復号してみない限り、媒体のどこにどのデータが記録されているかを制御部が認識することができず、きめ細かなトリックプレイが行えないという問題点がある。

【0016】

そこで、本発明の目的は、暗号化されて伝送されたコンテンツデータをそのまま記録媒体に記録し、さらにこのデータの暗号化に使用されたコンテンツキーをこの記録システムにおいて用いられる方法で暗号化して媒体に記録し、しかも、きめ細かなトリックプレイを行うことができるようにした情報記録／再生システム、情報記録装置及び情報再生装置を提供することにある。

【0017】

【課題を解決するための手段】

本発明では、記録機器が暗号化されて伝送されたコンテンツデータを記録する際に、コンテンツデータ自体は暗号化されたまま記録媒体に記録するが、コンテンツデータを復号して、再生時に必要な管理情報を集めたマップファイルを作成し、これをコンテンツデータとともに記録するようにすることで上記の課題を解決する。

【0018】

すなわち、本発明に係る情報記録／再生システムは、暗号化コンテンツ情報を

暗号化されたまま記録媒体に記録するコンテンツ情報記録手段と、上記暗号化コンテンツ情報からコンテンツ情報を暗号鍵により復号するコンテンツ情報復号手段と、上記暗号鍵を暗号化する暗号鍵暗号化手段と、上記暗号鍵暗号化手段により暗号化された暗号化暗号鍵を上記記録媒体に記録する暗号鍵記録手段と、上記コンテンツ情報復号手段により復号されたコンテンツ情報を用いて上記記録媒体に記録された暗号化コンテンツ情報を再生する際に必要となる管理情報を生成する管理情報生成手段と、上記管理情報生成手段により生成された管理情報を上記記録媒体に記録する記録手段とを備える情報記録装置と、上記情報記録装置により暗号化コンテンツ情報と暗号化暗号鍵と管理情報が記録された記録媒体から上記管理情報を読み出す管理情報読出手段と、上記記録媒体から上記暗号化暗号鍵を読み出す暗号鍵読出手段と、上記記録媒体から上記暗号化コンテンツ情報を読み出すコンテンツ情報読出手段と、上記管理情報読出手段により読み出された管理情報に基づいて上記記録媒体から暗号化暗号鍵と暗号化コンテンツ情報を読み出す位置を制御する読出位置制御手段と、上記暗号鍵読出手段により読み出された暗号化暗号鍵から暗号鍵を復号する暗号鍵復号手段とを備える情報再生装置とからなることを特徴とする。

【0019】

また、本発明に係る情報記録装置は、暗号化コンテンツ情報を暗号化されたまま記録媒体に記録するコンテンツ情報記録手段と、上記暗号化コンテンツ情報を復号するコンテンツ情報復号手段と、上記コンテンツ情報復号手段により暗号化コンテンツ情報から復号されたコンテンツ情報を用いて上記記録媒体に記録された暗号化コンテンツ情報を再生する際に必要となる管理情報を生成する管理情報生成手段と、上記管理情報生成手段により生成された管理情報を上記記録媒体に記録する記録手段とを備えることを特徴とする。

【0020】

さらに、本発明に係る情報再生装置は、暗号化コンテンツ情報と該暗号化コンテンツ情報からコンテンツ情報を復号するための暗号鍵を暗号化した暗号化暗号鍵と管理情報が記録された記録媒体から上記管理情報を読み出す管理情報読出手段と、上記記録媒体から上記暗号化暗号鍵を読み出す暗号鍵読出手段と、上記記

録媒体から上記暗号化コンテンツ情報を読み出すコンテンツ情報読出手段と、上記管理情報読出手段により読み出された管理情報に基づいて上記記録媒体から暗号化暗号鍵と暗号化コンテンツ情報を読み出す位置を制御する読出位置制御手段と、上記暗号鍵読出手段により読み出された暗号化暗号鍵から暗号鍵を第 1 の暗号鍵により復号する暗号鍵復号手段とを備えることを特徴する。

【0021】

【発明の実施の形態】

以下、本発明の実施の形態について、図面を参照しながら詳細に説明する。

【0022】

本発明は、例えば図 1 に示すような構成の光ディスク記録／再生装置 10 に適用される。

【0023】

この図 1 に示した光ディスク記録／再生装置 10 は、光ディスク 11 を回転駆動するスピンドルモータ 12、上記光ディスク 11 の情報記録面を光学的に走査する記録／再生ヘッド 13、上記記録／再生ヘッド 13 により得られる再生信号に基づいて上記スピンドルモータ 12 を制御するサーボ回路 14、上記記録／再生ヘッド 13 により上記光ディスク 11 を介してデータの記録／再生を行う記録／再生部 15、入力操作部 16 から入力される設定情報に基づいて上記サーボ回路 14 や記録／再生部 15 を制御する制御回路 17 等を備える。

【0024】

上記スピンドルモータ 12 は、サーボ回路 14 による制御に基づいて、上記光ディスク 11 を例えば線速度一定の状態で回転駆動させる。

【0025】

上記記録／再生ヘッド 13 は、上記スピンドルモータ 12 により回転駆動される光ディスク 11 の情報記録面を光学的に走査して、データの記録／再生を行う。

【0026】

上記サーボ回路 14 は、上記光ディスク 11 を所定の速度で（例えば線速度一定で）回転させるようにスピンドルモータ 12 を駆動するとともに、記録／再生

ヘッド 1 3 のトラッキング制御、フォーカシング制御やスレディング制御を行う。

【 0 0 2 7 】

上記記録／再生部 1 5 は、上記制御回路 1 7 により制御されて動作する暗号化処理部 4 と復号処理部 5 を有する。暗号化処理部 4 は、記録モード時に、外部から供給される記録信号を暗号化し、暗号化した記録信号を上記記録／再生ヘッド 1 3 に供給して、光ディスク 1 1 に記録させる。また、復号処理部 5 は、再生モード時に上記記録／再生ヘッド 1 3 により光ディスク 1 1 から再生された再生データを復号し、外部に再生信号として出力する。

【 0 0 2 8 】

上記入力操作部 1 6 は、図示しない操作ボタン、スイッチ、リモートコントローラなどにより構成され、ユーザにより入力操作されたとき、その入力操作に対応する信号を出力する。

【 0 0 2 9 】

上記制御回路 1 7 は、図示しないメモリに記憶されている所定のコンピュータプログラムに従って、装置全体を制御する。

【 0 0 3 0 】

この実施の形態において、光ディスク 1 1 は、図 2 に示すように、リードインエリア A R readin とデータエリア A R data からなる。

【 0 0 3 1 】

そして、光ディスク 1 1 のリードインエリア A R readin には、記録媒体の識別情報（以下、DiscID と称する）を記録システム共通の予め定められた方法で変換した（これを便宜上、本出願においては、“システム共通秘密で暗号化した”と呼ぶことにする）E DiscID と、ディスクキー K d をイフェクティブマスタキー K e m で暗号化した暗号化ディスクキー E K d が記録されている。

【 0 0 3 2 】

なお、媒体識別情報 DiscID を変換する方法すなわちシステム共通秘密は、著作権者から適正なライセンスを受ける際、後述するマスタキー K m とともに、ライセンスを受けた者に与えられる。

【 0 0 3 3 】

例えば、媒体識別情報DiscIDを変換する方法のひとつとして、所定のM系列符号に基づいて光ディスクの情報を表すピットのエッジの時間ずれとする方法がある。この場合、DiscIDをこのような方法で変換するということと、M系列符号がシステム共通秘密となり、媒体識別情報DiscIDはその両方がないと読み取る（復号する）ことができなくなる。

【 0 0 3 4 】

このようなM系列符号に基づく暗号化に関する技術は、特願平 9 - 2 8 8 9 6 0 号として本出願人が先に提案している。なお、この所定のシステム共通秘密は、著作権者から適正なライセンスを受ける際、後述するマスタキーK_mとともに、ライセンスを受けた者に与えられる。

【 0 0 3 5 】

イフェクティブマスタキーK_{em}は、式（1）に従い、マスタキーK_mとDiscIDの結合にhash関数を適用して計算される。

【 0 0 3 6 】

$$K_{em} = hash(K_m + DiscID) \quad (1)$$

ここで、マスタキーK_mは、著作権者等から適正にライセンスを受けた者（光ディスク記録再生装置）にだけ与えられる秘密のキーである。また、例えば、AとBの結合とは、それぞれが32ビットであるとき、Aの後方にBを結合して、64ビットのデータとすることを意味する。

【 0 0 3 7 】

また、光ディスク11のデータエリアARdataを構成する各セクタS_i（i = 1, 2, ...）は、ヘッダHD及びメインデータ部MDで構成され、ヘッダHDには、コンテンツキーK_cをディスクキーK_dで暗号化した暗号化コンテンツキーEK_cが格納されている（ここでS_iのiは、セクタの番号を示すが、特に個々のセクタを区別する必要がない場合は、iを省略する）。メインデータ部MDには、コンテンツデータをコンテンツキーK_cで暗号化した、すなわち伝送された記録機器で受信された暗号化コンテンツデータが格納されている。

【0038】

上記光ディスク記録／再生装置 10 における暗号化処理部 4 は、その具体的な構成を図 3 に示すように、DiscID 暗号化復号回路 4 1、K e m 発生モジュール 4 2、乱数発生回路 4 3、K d 暗号化復号回路 4 4、K c 暗号化回路 4 5 やコンテンツデータ復号回路 4 6、マップファイル生成回路 4 7 等からなる。

【0039】

上記 DiscID 暗号化復号回路 4 1 は、上記記録／再生ヘッド 1 3 により光ディスク 1 1 のリードインエリア A R readin から読み出された E DiscID を DiscID 暗号化復号回路 4 1 に含まれるシステム共通秘密に基づいて復号することにより、媒体識別情報 DiscID を生成する。また、この DiscID 暗号化復号回路 4 1 は、乱数発生回路 4 3 により発生された乱数を媒体識別情報 DiscID として受け取り、システム共通秘密に基づいて、上述したように暗号化して、E DiscID を生成する。この DiscID 暗号化復号回路 4 1 により上記乱数から生成された E DiscID は、上記記録／再生ヘッド 1 3 を介して光ディスク 1 1 のリードインエリア A R readin に記録される。

【0040】

上記 K e m 発生モジュール 4 2 は、マスターキー K m を記憶する K m メモリ 4 2 A と、上記マスターキー K m と媒体識別情報 DiscID とからイフェクティブマスターキー K e m を生成するハッシュ関数回路 4 2 B からなる。上記ハッシュ関数回路 4 2 B は、上述の (1) 式に従って、マスターキー K m と D i s c I D の結合を生成し、これに h a s h 関数を適用してイフェクティブマスターキー K e m を生成する。そして、上記ハッシュ関数回路 4 1 B は、生成したイフェクティブマスターキー K e m を K d 暗号化復号回路 4 4 に供給する。

【0041】

上記 K d 暗号化復号回路 4 4 は、上記記録／再生ヘッド 1 3 により光ディスク 1 1 のリードインエリア A R readin から読み出された暗号化ディスクキー E K d をイフェクティブマスターキー K e m で復号して、ディスクキー K d を生成する。また、この K d 暗号化復号回路 4 4 は、乱数発生回路 4 3 により発生された乱数をディスクキー K d として受け取り、イフェクティブマスターキー K e m で暗号化

して暗号化ディスクキー E K d を生成する。この K d 暗号化復号回路 4 4 により生成された暗号化ディスクキー E K d は、上記記録／再生ヘッド 1 3 を介して光ディスク 1 1 のリードインエリア A R readin に記録される。

【 0 0 4 2 】

上記 K c 暗号化回路 4 5 は、他の機器とのインタフェース部から受け取ったコンテンツキー K c をディスクキー K d で暗号化して暗号化コンテンツキー E K c を生成する。この K c 暗号化回路 4 5 により生成された暗号化コンテンツキー E K c は、上記記録／再生ヘッド 1 3 を介して光ディスク 1 1 のデータエリア A R data に記録される。

【 0 0 4 3 】

インタフェース部からわたされた暗号化されたコンテンツデータはそのまま上記記録／再生ヘッド 1 3 を介して光ディスク 1 1 のデータエリア A R data に記録される。

【 0 0 4 4 】

上記コンテンツデータ復号回路 4 6 は、コンテンツキー K c でコンテンツデータを復号し、マップファイル生成回路 4 7 に与える。

【 0 0 4 5 】

上記マップファイル生成回路 4 7 は、復号されたコンテンツデータから、再生時に必要な情報を集めたマップファイルを生成する。このマップファイル生成回路 4 7 により生成されたマップファイルは、上記記録／再生ヘッド 1 3 を介して光ディスク 1 1 のデータエリア A R data に記録される。

【 0 0 4 6 】

ここで、コンテンツデータが M P E G 2 トランスポートストリームである場合について、上記マップファイル生成回路 4 7 の具体的な構成例を示す図 4 のブロック図を参照して説明する。

【 0 0 4 7 】

このマップファイル生成回路 4 7 において、A V プログラムが多重化されている M P E G 2 トランスポートストリームが端子 4 7 1 を介して入力される P I D フィルター 4 7 2、上記 P I D フィルター 4 7 2 により取り出された P I D のト

ランスポートパケットがスイッチ 473 を介して供給される PAT/PMT 解析部 474 及びストリーム解析部 475 と、上記 PID フィルター 472 により取り出された PID のランスポートパケット供給されるカウンタ 476 と、上記 PAT/PMT 解析部 474 及びストリーム解析部 475 による各解析結果が与えられるマップデータ作成部 477 と、上記マップデータ作成部 477 に接続されたファイルシステム 478 等から成る。

【0048】

上記端子 471 を介して入力されるランスポートストリームは、ランスポートパケットが連続したストリームであり、ランスポートパケットは、MPEG2 ビデオストリームや MPEG1 オーディオストリームがパケット化されたものである。

【0049】

PID フィルター 472 は、入力されたランスポートストリームの中から指定された PID のランスポートパケットを取り出す。PID は、ランスポートパケットのヘッダの固定位置にある 13 ビット長の符号であり、そのランスポートパケットのペイロード（ランスポートパケットのヘッダに続くデータ部分）にストアされているデータのタイプを表す。

【0050】

はじめに PID フィルター 472 は、PID = 0x0000 である PAT (Program Association Table) のランスポートパケットを取り出す。PID フィルター 472 から出力される PAT のランスポートパケットは、スイッチ 473 から PAT/PMT 解析部 474 へ入力される。

【0051】

ここで、PAT/PMT 解析部 474 の動作について、図 5 に示すフローチャートを用いて説明する。

【0052】

ステップ S1 で、PAT/PMT 解析部 474 は、PAT のランスポートパケットを受信する。PAT には、ランスポートストリームに多重化されている AV プログラムの PMT (Program Map Table) のランスポートパケットの PI

Dが書かれている。

【0053】

ステップS2で、PAT/PMT解析部474はAVプログラムのPMTのPIDをPIDフィルターにセットする。PIDフィルター472は、PMTのPIDをもつトランスポート packets を取り出すと、それをPAT/PMT解析部474へ入力する。

【0054】

ステップS3で、PAT/PMT解析部474は、PMTのトランスポート packets を受信する。PMTには、AVプログラムを構成するビデオストリームやオーディオストリームをペイロードに持つトランスポート packets のPIDが書かれている。PAT/PMT解析部474は、AVプログラムを構成するビデオストリームやオーディオストリームをペイロードに持つトランスポート packets のPIDを取得する。

【0055】

ステップS4で、PAT/PMT解析部474は、AVプログラムを構成するビデオストリームやオーディオストリームをペイロードに持つトランスポート packets のPIDをPIDフィルターとストリーム解析部475にセットして、動作を終了する。

【0056】

そして、上記PAT/PMT解析部474は、マップデータ作成部477へ次のパラメータを与える。

【0057】

- (A) AVプログラムのPMTのトランスポート packets のPID
- (B) AVプログラムを構成するビデオのトランスポート packets のPID及びビデオのstream_type
- (C) AVプログラムを構成するオーディオのトランスポート packets のPID及びオーディオのstream_type
- (D) AVプログラムのPCR_PID

ここで、stream_typeとは、PMTに書いてある内容であり、ビデ

オの場合、MPEG2/MPEG1などのストリームタイプを表し、またオーディオの場合、MPEG1/AC-3などのストリームタイプを表す。

【0058】

そして、PIDフィルター472は、PAT/PMT解析部474から指定されたビデオのトランスポートパケットとオーディオのトランスポートパケットを入力トランスポートストリームの中から取り出すと、それをスイッチ473を介してストリーム解析部475へ入力する。ビデオのトランスポートパケットとオーディオのトランスポートパケット以外のトランスポートパケット（サービスインフォメーションのパケットなど）は、ストリーム解析部475へ入力されない。

【0059】

PIDフィルター472から出力されるトランスポートパケットは、カウンタ476へ入力される。カウンタ475は、記録するトランスポートストリームの先頭パケットから現在のパケットまでのバイト数を計算し、その値をストリーム解析部475に与える。

【0060】

ストリーム解析部475は、AVプログラム中のランダムアクセス再生できるポイントを抽出する。ビデオデータのランダムアクセスポイントのトランスポートパケットは、MPEGビデオのシーケンスヘッダとそれに続くIピクチャデータをペイロードに持つパケットである。ビデオデータのランダムアクセスポイントリストの概念図を図6に示す。ランダムアクセスポイントは、ランダムアクセスするトランスポートパケットのタイムスタンプとデータ読み出し開始のアドレスを表す。ここで、タイムスタンプは、ランダムアクセスポイントのトランスポートパケットの記録器への入力時刻、又は、ランダムアクセスポイントのIピクチャのPTS (Presentation Time Stamp) に基づいて計算される。PTSは、MPEG2システムズ規格のPESパケットのヘッダに付加されている情報である。なお、この図6ではトランスポートストリームファイルをトランスポートパケットが連続して記録されている形で示しているが、トランスポートパケット毎に、そのパケットの記録器への入力時刻を示すタイムスタンプを付加して記録して

も良い。このタイムスタンプは、例えば、DVフォーマットで規定されているところのトランスポート packets に付加される 4 バイト長の T S P _ e x t r a _ h e a d e r と同様なものである。

【 0 0 6 1 】

ビデオデータ及びオーディオデータのランダムアクセスポイント情報は、マップデータ作成部 4 7 7 に与えられる。マップデータ作成部 4 7 7 は、ランダムアクセスポイント情報をテーブル化する。

【 0 0 6 2 】

マップデータ作成部 4 7 7 は、マップデータテーブルをファイルシステム 4 7 8 に与える。

【 0 0 6 3 】

ファイルシステム 4 7 8 は、マップデータテーブルをファイル化して出力する。

【 0 0 6 4 】

図 7 は、トランスポートストリームとマップファイルの説明図である。マップファイルは、次のデータを持つ。

【 0 0 6 5 】

1. AVプログラムの PMT のトランスポート packets の P I D
2. AVプログラムを構成するビデオのトランスポート packets の P I D 及びビデオの s t r e a m _ t y p e
3. AVプログラムを構成するオーディオのトランスポート packets の P I D 及びオーディオの s t r e a m _ t y p e
4. AVプログラムの P C R _ P I D
5. AVビデオのランダムアクセスポイントのリスト
6. AVオーディオのランダムアクセスポイントのリスト

上記光ディスク記録／再生装置 1 0 における復号処理部 5 は、その具体的な構成を図 8 に示すように、E D i s c I D 復号回路 5 1、K e m 発生モジュール 5 2、K d 復号回路 5 4、K c 復号回路 5 5 等からなる。

【0066】

EDiscID復号回路51は、上記記録／再生ヘッド13により光ディスク11のリードインエリアARreadinから読み出されたEDiscIDを自身が持つシステム共通秘密に基づいて復号して、媒体識別情報DiscIDを生成する。このEDiscID復号回路51は、生成した媒体識別情報DiscIDをKem発生モジュール52に与える。

【0067】

Kem発生モジュール52は、マスターキーKmを記憶するKmメモリ52Aと、上記マスターキーKmと媒体識別情報DiscIDとからイフェクティブマスターキーKemを生成するハッシュ関数回路52Bからなる。上記ハッシュ関数回路52Bは、上述の(1)式に従って、マスターキーKmとDiscIDの結合を生成し、これにhash関数を適用してイフェクティブマスターキーKemを生成する。そして、上記ハッシュ関数回路41Bは、生成したイフェクティブマスターキーKemをKd復号回路54に供給する。このKem発生モジュール52は、上述のKem発生モジュール42と同一の構成とし、両者を兼用するようにしてもよい。

【0068】

EKd復号回路54は、上記記録／再生ヘッド13により光ディスク11のリードインエリアARreadinから読み出された暗号化ディスクキーEKdをイフェクティブマスターキーKemで復号して、ディスクキーKdを算出する。

【0069】

EKc復号回路55は、光ディスク11のデータエリアARdataから上記記録／再生ヘッド13により読み出される各セクタSiのヘッダに記録されている暗号化コンテンツキーEKcをディスクキーKdで復号して、コンテンツキーKcを算出する。

【0070】

なお、図8に示した復号処理部5では、暗号化されたまま読み出されたコンテンツデータと復号したコンテンツキーKcとを、データインタフェース部に渡すようになっている。これは例えば、このコンテンツを他の機器に伝送するような

場合に用いられる。

【 0 0 7 1 】

これに対し、図 9 に示す復号処理部 5 は、光ディスク 1 1 のデータエリア A R data から上記記録／再生ヘッド 1 3 により読み出された暗号化コンテンツデータを E K c 復号回路 5 5 で復号したコンテンツキー K c により復号して平文コンテンツデータを生成するコンテンツ復号回路 5 6 を備えている。

【 0 0 7 2 】

この図 9 に示す復号処理部 5 は、例えば、この再生機器においてこの後コンテンツデータに施されている M P E G などの符号が復号され、D / A コンバータを通して画像として出力される場合に用いられる。

【 0 0 7 3 】

なお、この再生処理を行う際に、記録時に作成されたマップファイルに含まれる情報を用いて、制御回路 1 7 により光ディスク 1 1 からのコンテンツデータの読み出しを制御する。

【 0 0 7 4 】

図 1 0 は、マップファイルに含まれる情報を用いてコンテンツデータの読み出しを制御するコンテンツデータ再生装置のブロック図を示す。ここでは、上述の図 4 で説明したマップファイル生成回路 4 7 で作成したマップファイルの情報を用いて、そのマップファイルに対応するトランスポートストリームファイルの読み出しを制御するトランスポートストリーム再生装置を説明する。

【 0 0 7 5 】

記録媒体 6 0 には、トランスポートストリームファイルとそのマップファイルが記録されている。

【 0 0 7 6 】

再生制御部 6 5 は、読み出し制御部 6 1 に対して、マップファイルを読み出すように指示する。そして、読み出し制御部 6 1 は、記録媒体 6 0 からマップファイルを読み出し、復調部 6 2、誤り訂正部 6 3、ファイルシステム部 6 4 の処理を経て、再生制御部 6 5 へマップファイルを入力する。

【0077】

再生制御部 65 は、AV プログラムの PMT のトランスポートパケットの P I D、プログラムを構成するビデオデータのトランスポートパケットの P I D、ビデオデータの `stream_type`、プログラムを構成するオーディオデータのトランスポートパケットの P I D、オーディオデータの `stream_type`、PCR_P I D を図示しないデマルチプレクサと AV デコーダへ供給する。

【0078】

ユーザーインタフェースによってランダムアクセス再生を指示された場合、再生制御部 65 は、内部に記憶されているマップデータの内容に基づいて、記憶媒体 60 からのデータの読み出し位置を決定し、ランダムアクセス制御情報を読み出し制御部 61 へ入力する。例えば、ユーザーによって選択されたプログラムをある時刻から途中再生をする場合、再生制御部 65 は、タイムスタンプのリストから指定された時刻にもっとも近いタイムスタンプを見つけ出し、そのタイムスタンプに対応するトランスポートストリームのアドレスにある I ピクチャからデータを読み出すように読み出し制御部 61 へ指示する。また、ユーザーによって選択されたプログラムを高速再生をする場合、再生制御部 65 は、そのプログラムに対応するランダムアクセスポイントのデータに基づいて、プログラムの中の I ピクチャデータを順次連続して読み出すように読み出し制御部 61 へ指示する。

【0079】

読み出し制御部 61 は、指定されたランダムアクセスポイントからデータを読み出し、読み出されたデータは、復調部 62、誤り訂正部 63、ファイルシステム部 64 の処理を経て、トランスポートストリームを出力する。

【0080】

次に、ユーザデータが光ディスク 11 に記録される場合の暗号化処理部 4 における処理手順を、図 11 のフローチャートを参照して説明する。なお、この例の場合、媒体識別情報 DiscID は、光ディスク 11 製造時に、光ディスク 11 に書き込まれているものとする。

【 0 0 8 1 】

最初に、ステップ S 1 1 において、DiscID暗号化復号回路 4 1 は、光ディスク 1 1 のリードインエリアから読み出された、暗号化されている媒体識別情報Disc IDである E DiscIDを受け取る。DiscID暗号化復号回路 4 1 は、さらに、ステップ S 1 2 において、自身が持っているシステム共通秘密に基づいて、E DiscIDを復号して、DiscIDを生成し、K e m発生モジュール 4 2 のハッシュ関数回路 4 2 E に出力する。システム共通秘密は、著作権者から適正なライセンスを受けるときに、与えられたものである。

【 0 0 8 2 】

ステップ S 1 3 において、K e m発生モジュール 4 2 のハッシュ関数回路 4 2 Bは、K e m発生モジュール 4 2 のK mメモリ 4 2 AからマスターキーK mを読み出す。K e m発生モジュール 4 2 のハッシュ関数回路 4 2 Bは、さらに、ステップ S 1 4 で、上述の式 (1) に従い、光ディスク 1 1 の媒体識別情報DiscIDとマスターキーK mの結合にh a s h関数を適用して、イフェクティブマスターキーK e mを計算し、K d暗号化復号回路 4 4 に供給する。

【 0 0 8 3 】

次に、ステップ S 1 5 において、K d暗号化復号回路 2 6 は、光ディスク 1 1 のリードインエリアから読み出された暗号化ディスクキーE K dを受け取る。K d暗号化復号回路 2 6 は、ステップ S 3 6 で、光ディスク 1 1 のリードインエリアに、暗号化ディスクキーE K dが書き込まれているか否か（暗号化ディスクキーE K dを受け取ることができたか否か）の判定を行う。暗号化ディスクキーE K dが書き込まれていないと判定された場合、ステップ S 3 7 に進み、乱数発生回路 4 3 は、dビット、具体的には例えば5 6ビットの乱数を発生し、ディスクキーK dとして、K d暗号化復号回路 4 4 に出力する。

【 0 0 8 4 】

次に、ステップ S 1 8 において、K d暗号化復号回路 4 4 は、乱数発生回路 4 3 から供給されたディスクキーK dをハッシュ関数回路 4 2 Bから受け取ったイフェクティブマスターキーK e mにより暗号化して、暗号化ディスクキーE K dを生成し、光ディスク 1 1 のリードインエリアに記録する。

【 0 0 8 5 】

ステップ S 1 6 で、暗号化ディスクキー E K d が書き込まれていると判定された場合、ステップ S 1 9 に進み、K d 暗号化復号回路 4 4 は、この光ディスク 1 1 のリードインエリア A k r e a d i n から読み出された暗号化ディスクキー E K d をハッシュ関数回路 4 2 B から受け取ったイフェクティブマスタキー K e m で復号して、ディスクキー K d を得る。K d 暗号化復号回路 4 4 は、そのディスクキー K d を、K c 暗号化回路 4 5 に出力する。

【 0 0 8 6 】

ステップ S 1 8 又は S 1 9 の処理の後、ステップ S 2 0 で、K c 暗号化回路 4 5 は、インタフェース部からコンテンツキー K c と暗号化コンテンツデータを受け取り、ステップ S 2 1 でコンテンツキー K c を K d 暗号化復号回路 4 4 (暗号化ディスクキー E K d が光ディスク 1 1 に記録されている場合)、又は乱数発生回路 4 3 (暗号化ディスクキー E K d が光ディスク 1 1 に記録されていない場合) から受け取ったディスクキーで暗号化して暗号化コンテンツキー E K c を生成する。K c 暗号化回路 4 5 は、また、その暗号化コンテンツキー E K c を、光ディスク 1 1 のデータエリアにあるセクタヘッドに記録する。

【 0 0 8 7 】

次に、ステップ S 2 2 において、コンテンツデータを光ディスク 1 1 のデータエリアのメインデータ部に記録する。

【 0 0 8 8 】

ステップ S 2 3 において、コンテンツデータ復号回路 4 6 は、インタフェース部から受け取ったコンテンツキー K c を用いて暗号化コンテンツデータを復号し、平文のコンテンツデータを生成してマップファイル生成回路 4 7 にわたす。

【 0 0 8 9 】

ステップ S 2 4 において、マップファイル生成回路 4 7 は、(もしマップファイルがなければあらたに生成し、) 平文コンテンツデータから再生時に必要となる情報を抜き出してマップファイルに追加する。

【 0 0 9 0 】

上述のマップファイル生成回路 4 7 のストリーム解析部 4 7 5 の動作例を図 1

2と図13のフローチャートを用いて説明する。図12は、ビデオデータのトランスポートパケットの解析動作を説明するものであり、また、図13は、オーディオデータのトランスポートパケットの解析動作を説明するものである。

【0091】

先ず、図12に示すフローチャートを参照して、ビデオデータのトランスポートパケットの解析動作を説明をする。

【0092】

ステップS31において、ストリーム解析部475は、記録するAVプログラムのビデオのPIDとそのstream_typeがPAT/PMT解析部474によって入力される。

【0093】

ステップS32において、ストリーム解析部475は、ビデオデータのトランスポートパケットを受信する。ストリーム解析部475にはビデオバッファが内蔵されている。ストリーム解析部475は、ビデオデータのトランスポートパケットを受信すると、そのペイロードをビデオストリームバッファへ入力する。

【0094】

ステップS33において、ストリーム解析部475は、ビデオストリームバッファの中のストリームにMPEGビデオのsequence_header_code(32ビット長で"0x000001B3"の符号)が含まれるか否かを調べる。具体的には、バッファ内のストリームの先頭から1バイトずつシフトしてsequence_header_codeとマッチングするか否かを調べる。検査の終わったバイトは、ビデオストリームバッファから捨てる。

【0095】

ステップS33でストリームにsequence_header_codeが含まれていない時は、ステップS32へ戻る。ステップS32が2回目以降である場合は、ビデオパケットのペイロードをビデオバッファの最後のデータへ追加入力(append)する。

【0096】

ステップS33でストリームにsequence_header_codeが含まれていた時は、ステップS34において、sequence_header_codeの第1バイト目を含むトランスポ

ートパケットをランダムアクセスする時の I ピクチャデータの読み出し開始ポイントとする。

【0097】

ステップ S 3 5 において、ストリーム解析部 4 7 5 は、上記パケットの読み出しの開始ポイントをマッピングデータ作成部 4 7 7 へ知らせる。マッピングデータ作成部 4 7 7 へは、ランダムアクセスポイントのアドレスとして記録するトランスポートストリームの先頭からそのパケットまでのバイト数が、カウンタ部 4 7 6 から入力され、またランダムアクセスポイントのタイムスタンプとして、そのパケットのペイロードに含まれる I ピクチャの P T S (Presentation Time Stamp) が入力される。

【0098】

ステップ S 3 6 において、ストリーム解析部 4 7 5 は、現在のパケットが最後の入力パケットであるかどうかを判定する。最後のパケットでない場合、ステップ S 3 2 へ戻る。最後のパケットである場合、処理を終了する。

【0099】

次に、図 1 3 を用いてオーディオデータのトランスポートパケットの解析動作を説明をする。

【0100】

ステップ S 4 1 において、ストリーム解析部 4 7 5 は、記録するプログラムのオーディオデータの P I D とその stream_type が PAT/PMT 解析部 4 7 4 によって入力される。

【0101】

ステップ S 4 2 において、ストリーム解析部 4 7 5 は、オーディオデータのトランスポートパケットを受信する。

【0102】

ステップ S 4 3 において、ストリーム解析部 4 7 5 は、ペイロードのオーディオストリームの中にオーディオフレームの第 1 バイト目の sync_byte が含まれるかを調べる。オーディオフレームは符号化ビットレートにより決まる固定長であるので、この固定長間隔で現れる sync_byte がペイロードに含まれるかどうかを

調べる。

【0 1 0 3】

ステップ S 4 3 でペイロードにオーディオフィレームの sync_byte が含まれていない時は、ステップ S 4 2 へ戻る。

【0 1 0 4】

ステップ S 4 3 でペイロードにオーディオフィレームの sync_byte が含まれていた時は、ステップ S 4 4 へ進む。

【0 1 0 5】

ステップ S 4 4 において、ストリーム解析部 4 7 5 は、オーディオフィレームの sync_byte を含むパケットをランダムアクセスする時のオーディオフィレームの読み出し開始ポイントであることをマップデータ作成部 4 7 7 へ知らせる。マップデータ作成部 4 7 7 へは、ランダムアクセスポイントのアドレスとして記録するトランスポートストリームの先頭からそのパケットまでのバイト数が、カウンタ部 4 7 6 から入力され、またランダムアクセスポイントのタイムスタンプとして、そのパケットのペイロードに含まれるオーディオフィレームの P T S (Presentation Time Stamp) が入力される。

【0 1 0 6】

ステップ S 4 5 において、ストリーム解析部 4 7 5 は、現在のパケットが最後の入力パケットであるかどうかを判定する。最後のパケットでない場合、ステップ S 4 2 へ戻る。最後のパケットである場合、処理を終了する。

【0 1 0 7】

そして、図 1 1 に示したフローチャートのステップ S 2 5 において、暗号化処理部 4 の各回路は、すべてのコンテンツデータを記録したか否かの判定を行う。すべてのコンテンツデータがまだ記録されていないと判定された場合、ステップ S 2 6 に進み、暗号化処理部 4 の各回路は、光ディスク 1 1 のまだデータを記録していないセクタにアクセスし、ステップ S 2 0 に戻り、以下同様の処理を繰り返す。ステップ S 4 5 で、すべてのコンテンツデータが記録されたと判定された場合、暗号化処理部 4 の各回路は、すべての記録処理を終了する。

【0108】

以上のようにして、著作権者から適正なライセンスを受けるときに、与えられた所定のシステム共通秘密で、暗号化されたDiscIDを復号し、媒体識別情報DiscIDを得ることにより、暗号化した情報が記録媒体に記録される。

【0109】

次に、製造時に、媒体識別情報DiscIDが記録されていない光ディスク11に対して、ユーザデータを記録する場合の暗号化処理部4における処理手順を、図14のフローチャートを参照して説明する。

【0110】

最初に、ステップS51において、DiscID暗号化復号回路21は、光ディスク11のリードインエリアARreadinから読み出されたEDiscIDを受け取り、またKd暗号化復号回路44は、光ディスク11のリードインエリアARreadinから読み出された暗号化ディスクキーEKdを受け取る。

【0111】

次に、ステップS52において、DiscID暗号化復号回路41は、光ディスク11のリードインエリアARreadinにEDiscIDが書き込まれているか否か（EDiscIDを受けることができたか否か）の判定を行い、Kd暗号化復号回路44は、光ディスク11のリードインエリアARreadinに暗号化ディスクキーEKdが書き込まれているか否か（暗号化ディスクキーEKdを受け取ることができたか否か）の判定を行う。EDiscIDと暗号化ディスクキーEKdが共に書き込まれていないと判定された場合、ステップS53に進み、乱数発生回路43は、1ビット、具体的には例えば128ビットの乱数を発生し、媒体識別DiscIDとして、DiscID暗号化復号回路41に出力する。

【0112】

次に、ステップS54において、DiscID暗号化復号回路41は、乱数発生回路43から供給された媒体識別情報DiscIDを、自身で持っているシステム共通秘密に基づいて暗号化して、EDiscIDを生成し、光ディスク11のリードインエリアARreadinに記録する。

【0113】

次に、ステップS55において、K_{em}発生モジュール42のハッシュ関数回路42Bは、K_{em}発生モジュール42のK_mメモリ42Aから、マスターキーK_mを読み出す。K_{em}発生モジュール42のハッシュ関数回路42Bは、ステップS56で、上述の式(1)に従い、光ディスク11の媒体識別情報DiscID、及びK_mメモリ42Aから読み出したマスターキーK_mの結合にh_as_h関数を適用して、イフェクティブマスターキーK_{em}を計算し、K_d暗号化復号回路44に供給する。

【0114】

次に、ステップS57において、乱数発生回路43は、dビット、具体的には例えば56ビットの乱数を発生し、ディスクキーK_dとして、K_d暗号化復号回路44に出力する。K_d暗号化復号回路44は、ステップS58において、乱数発生回路43から供給されたディスクキーK_dを、ハッシュ関数回路42Bから受け取ったイフェクティブマスターキーK_{em}により暗号化して、暗号化ディスクキーE_{K_d}を生成し、光ディスク11のリードインエリアAR_{readin}に記録する。

【0115】

ステップS52で、E_{DiscID}と暗号化ディスクキーE_{K_d}が書き込まれていると判定された場合、ステップS59に進み、DiscID暗号化復号回路41は、この光ディスク11から読み出されたE_{DiscID}を、自身が持っているシステム共通秘密で復号して、媒体識別情報DiscIDを生成する。

【0116】

ステップS60において、K_{em}発生モジュール42のハッシュ関数回路42Bは、K_{em}発生モジュール42のK_mメモリ42Aから、マスターキーK_mを読み出す。K_{em}発生モジュール42のハッシュ関数回路42Bは、ステップS61で、上述の式(1)に従い、光ディスク11のDiscIDとマスターキーK_mの結合にh_as_h関数を適用して、イフェクティブマスターキーK_{em}を計算し、K_d暗号化復号回路44に供給する。

【0 1 1 7】

次に、ステップ S 6 2 において、K d 暗号化復号回路 4 4 は、この光ディスク 1 1 から読み出された暗号化ディスクキー E K d を、ハッシュ関数回路 4 2 B から受け取ったイフェクティブマスタキー K e m で復号して、ディスクキー K d を得る。K d 暗号化復号回路 2 4 4、ディスクキー K d を K c 暗号化回路 4 5 に出力する。

【0 1 1 8】

ステップ S 5 8 又はステップ S 6 2 の処理の後は、ステップ S 6 3 に進むが、ステップ S 6 3 乃至ステップ S 7 0 で行われる処理は、図 1 1 のステップ S 2 0 乃至ステップ S 2 7 で行われる処理と同様の処理であり、すべてのコンテンツデータが記録されたと判定された場合、すべての記録処理が終了する。

【0 1 1 9】

以上のようにして、媒体識別情報 DiscID が生成され、記録媒体に記録され、そして生成された媒体識別情報 DiscID とマスタキー K m に対応して暗号化されたコンテンツデータが記録媒体に記録される。このことより、例えば、既存の記録媒体（DiscID が記録されていない記録媒体）に複製されたコンテンツデータを、著作権者から適正にライセンスを受けていない者は、意味のある情報として再生することができない。

【0 1 2 0】

次に、図 1 5 のフローチャートを参照して、復号処理部 5 により行われるユーザデータの再生処理を説明する。最初に、ステップ S 8 1 において、E DiscID 復号回路 5 1 は、光ディスク 1 1 のリードインエリア A R readin から読み出された、暗号化された媒体識別情報 DiscID である E DiscID を受け取る。E DiscID 復号回路 5 1 はさらに、ステップ S 8 2 において、自身が持つシステム共通秘密に基づいて、E DiscID を復号して媒体識別情報 DiscID を生成し、K e m 発生モジュール 5 2 のハッシュ関数回路 5 2 B に出力する。

【0 1 2 1】

次に、ステップ S 8 3 において、K e m 発生モジュール 5 2 のハッシュ関数回路 5 2 B は、E DiscID 復号回路 5 1 から出力された媒体識別情報 DiscID を受け取

るとともに、K mメモリ 5 2 AからマスターキーK mを読み出し、上述の式(1)に従い、光ディスク 1 1の媒体識別情報DiscIDとマスターキーK mの結合にh a s h関数を適用してイフェクティブマスターキーK e mを算出し、E K d復号回路 5 4に供給する。

【0 1 2 2】

ステップS 8 4において、E K d復号回路 5 4は、光ディスク 1 1のリードインエリアA R readinから読み出された暗号化ディスクキーE K dを受け取る。E K d復号回路 5 4は、ステップS 8 5で、この読み出された暗号化ディスクキーE K dを、ハッシュ関数回路 5 2 Bから受け取ったイフェクティブマスターキーK e mで復号して、ディスクキーK dを算出し、E K c復号回路 5 5に出力する。

【0 1 2 3】

次に、ステップS 8 6において、制御回路 1 7はマップファイルを光ディスク 1 1から読み出し、これを用いてコンテンツデータの読み出し場所を決める。

【0 1 2 4】

ステップS 8 7において、E K c復号回路 5 5は、光ディスク 1 1のデータエリアA R dataから読み出された各セクタの暗号化コンテンツキーE K cを受け取る。E K c復号回路 5 5は、ステップS 8 8で、この読み出された暗号化コンテンツキーE K cを、E K d復号回路 5 4から受け取ったディスクキーK dで復号して、コンテンツキーK cを算出し、ステップS 8 9でインタフェース部にわたす。

【0 1 2 5】

ステップS 9 0で、光ディスク 1 1のデータエリアA R dataから暗号化されたコンテンツデータを読み出してインタフェース部にわたす。

【0 1 2 6】

次に、ステップS 9 1において、復号部 5の各回路は、光ディスク 1 1のデータエリアA R dataから、必要なすべてのコンテンツデータを読み出したか否かの判定を行う。すべてのコンテンツデータがまだ読み出されていないと判定された場合、ステップS 9 2に進み、復号部 5の各回路は、光ディスク 1 1の、まだ読み出されていない次のセクタのデータの供給を受け、ステップS 8 6以降の処理

を繰り返す。必要なすべてのコンテンツデータが読み出されたと判定された場合、復号部 5 の各回路は、すべての再生処理を終了する。

【0 1 2 7】

以上は、図 8 に示したように、暗号化されたまま読み出されたコンテンツデータと、復号したコンテンツキー Kc とを、データインタフェース部に渡すようになっている場合の処理である。

【0 1 2 8】

これは例えば、このコンテンツを他の機器に伝送するような場合に用いられる。

【0 1 2 9】

これに対し、図 9 に示した復号処理部 5 のように、コンテンツ復号回路 5 6 において、光ディスク 1 1 のデータエリア A R data から上記記録／再生ヘッド 1 3 により読み出された暗号化コンテンツデータを E K c 復号回路 5 5 で復号したコンテンツキー K c により復号して平文コンテンツデータを生成する場合の処理例を、図 1 6 のフローチャートを用いて説明する。

【0 1 3 0】

これは例えば、この再生機器においてこの後コンテンツに施されている M P E G などの符号が復号され、D / A コンバータを通して画像として出力される場合に用いられる。

【0 1 3 1】

図 1 6 に示したフローチャートにおけるステップ S 1 0 1 乃至ステップ S 1 0 8 は、図 1 5 に示したフローチャートにおけるのステップ S 8 1 乃至ステップ S 8 8 と同じ処理であるので説明を省略する。

【0 1 3 2】

ステップ S 1 0 9 で、コンテンツ復号回路 5 6 は、光ディスク 1 1 から読み出した、暗号化されているコンテンツデータを、E K c 復号回路 5 5 からわたされたコンテンツキー K c を用いて復号し、平文コンテンツデータを生成してこれを例えばこの光ディスクプレーヤーが持つ M P E G デコーダーなどに出力する。

【0133】

ステップS110において、復号部5の各回路は、光ディスク11のデータエリアARdataから、必要なすべてのコンテンツデータを読み出したか否かの判定を行う。すべてのコンテンツデータがまだ読み出されていないと判定された場合、ステップS111に進み、復号部5の各回路は、光ディスク11の、まだ読み出されていない次のセクタのデータの供給を受け、ステップS106以降の処理を繰り返す。必要なすべてのコンテンツデータが読み出されたと判定された場合、復号部5の各回路は、すべての再生処理を終了する。

【0134】

このように、記録媒体のIDを生成し、所定のシステム共通秘密で暗号化して、記録媒体に記録することで、著作権者から適正にライセンスを受けた者だけが、その記録媒体にアクセスできるようにする。

【0135】

上記実施例において、コンテンツデータ及び暗号化コンテンツキーEKcを、光ディスクのセクタごとに記録、再生するようにしているが、このセクタは光ディスクの物理セクタに必ずしも一致する必要はなく、幾つかの物理セクタ若しくは論理セクタを合わせたものなどあらかじめ定められた範囲であるとか、記録時ごとに決められる範囲であってもよい。

【0136】

また、上記実施の形態において、ディスクキーKdは光ディスク一枚につきひとつずつ使用されるようになっているが、これについてもひとつである必要はなく、あらかじめ定められた光ディスクのブロックごとにひとつずつ使用したり、記録時ごとにひとつずつ使用してもよい。

【0137】

さらに、上記実施の形態においてマップファイルをコンテンツキーやディスクキーで暗号化して光ディスクに記録してもよい。

【0138】

本発明は、光ディスク以外の記録媒体にデータを記録又は再生する場合にも適用が可能である。

【0 1 3 9】

【発明の効果】

以上のように、本発明によれば、記録機器が暗号化されて伝送されたコンテンツデータを記録する際に、コンテンツデータ自体は暗号化されたまま記録媒体に記録するが、コンテンツデータを復号して、再生時に必要な情報を集めたマップファイルを作成し、これをコンテンツデータとともに記録するようにすることで、再生時に必要な情報を持たない方法に比べて、きめ細かなトリックプレイを行える。

【図面の簡単な説明】

【図 1】

本発明を適用した光ディスク記録／再生装置の構成を示すブロック図である。

【図 2】

上記光ディスクに記録されたデータの構造を模式的に示す図である。

【図 3】

上記光ディスク記録／再生装置における暗号化処理部の具体的な構成を示すブロック図である。

【図 4】

上記暗号化処理部のマップファイル生成回路の具体的な構成例を示すブロック図である。

【図 5】

上記マップファイル生成回路の P A T / P M T 解析部の動作を示すフローチャートである。

【図 6】

M P E G 方式におけるビデオデータのランダムアクセスポイントリストの概念図である。

【図 7】

トランスポートストリームとマップファイルの説明図である。

【図 8】

上記光ディスク記録／再生装置における復号処理部の具体的な構成例を示すブ

ロック図である。

【図 9】

上記復号処理部の他の構成例を示すブロック図である。

【図 1 0】

マップファイルに含まれる情報を用いてコンテンツデータの読み出しを制御するコンテンツデータ再生装置の構成を示すブロック図である。

【図 1 1】

ユーザデータが光ディスクに記録される場合の暗号化処理部における処理手順を示すフローチャートである。

【図 1 2】

上記マップファイル生成回路のストリーム解析部によるビデオデータのトランスポートパケットの解析動作を示すフローチャートである。

【図 1 3】

上記ストリーム解析部によるオーディオデータのトランスポートパケットの解析動作を示すフローチャートである。

【図 1 4】

製造時に、媒体識別情報DiscIDが記録されていない光ディスクに対して、ユーザデータを記録する場合の暗号化処理部における処理手順を示すフローチャートである。

【図 1 5】

上記復号処理部により行われるユーザデータの再生処理を示すフローチャートである。

【図 1 6】

上記復号処理部により行われるユーザデータの再生処理を示すフローチャートである。

【符号の説明】

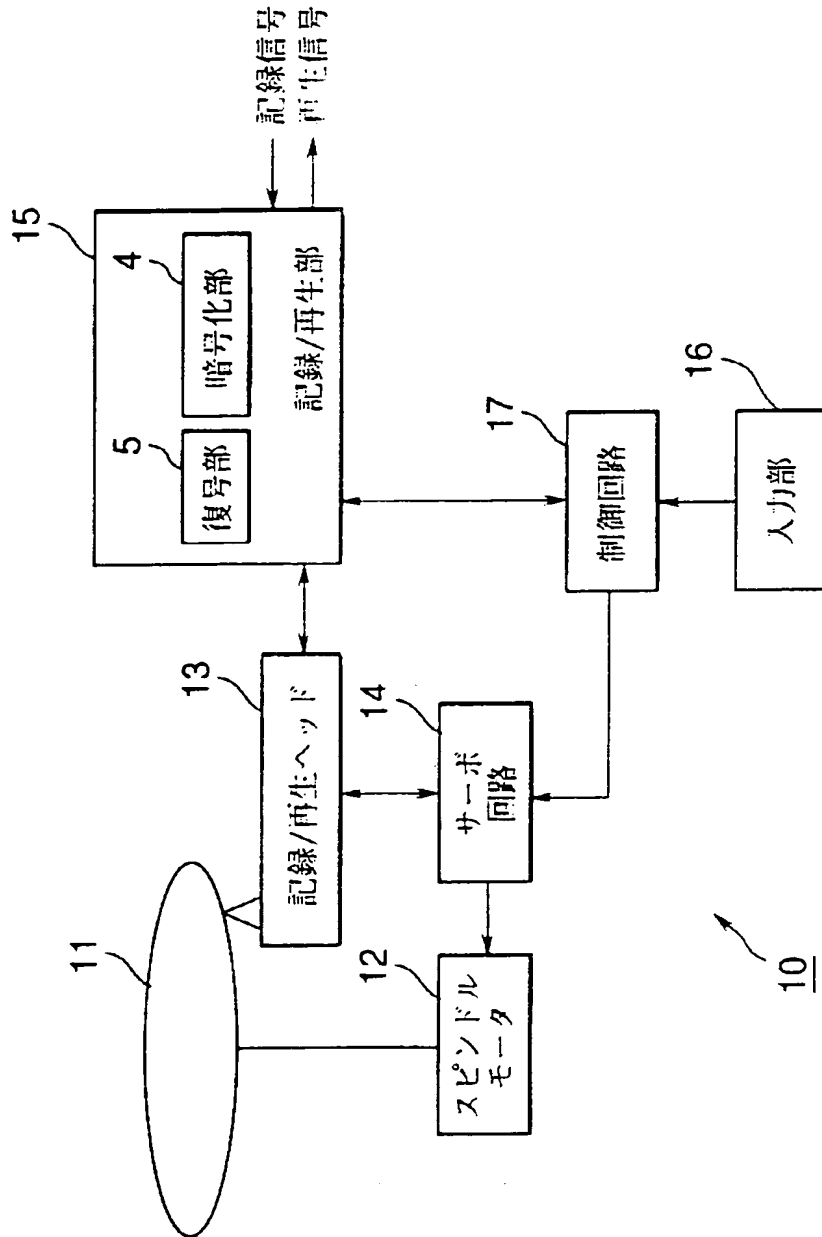
4 暗号化処理部、5 復号処理部、1 0 光ディスク記録／再生装置、1 1 光ディスク、1 2 スピンドルモータ、1 3 記録／再生ヘッド、1 4 サーボ回路、1 5 記録／再生部、1 6 入力操作部、1 7 制御回路、4 1 Disc

ID暗号化復号回路、42 Kem発生モジュール、43 乱数発生回路、44
Kd暗号化／復号回路、45 Kc暗号化回路、46 コンテンツデータ復号回
路、47 マップファイル生成回路47、51 EDiscID復号回路、52 Ke
m発生モジュール、54 Kd復号回路、55 Kc復号回路、56 コンテン
ツ復号回路

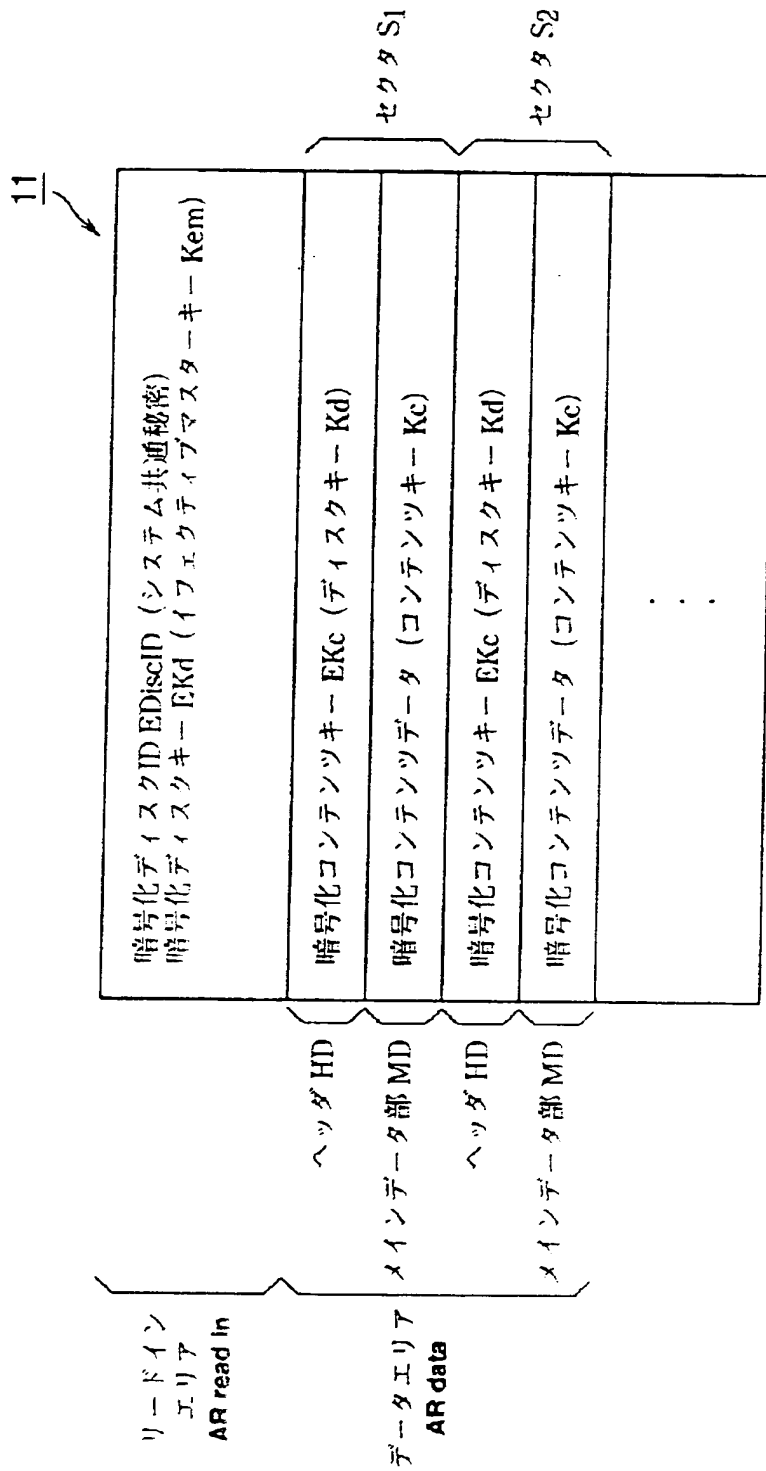
【書類名】

図面

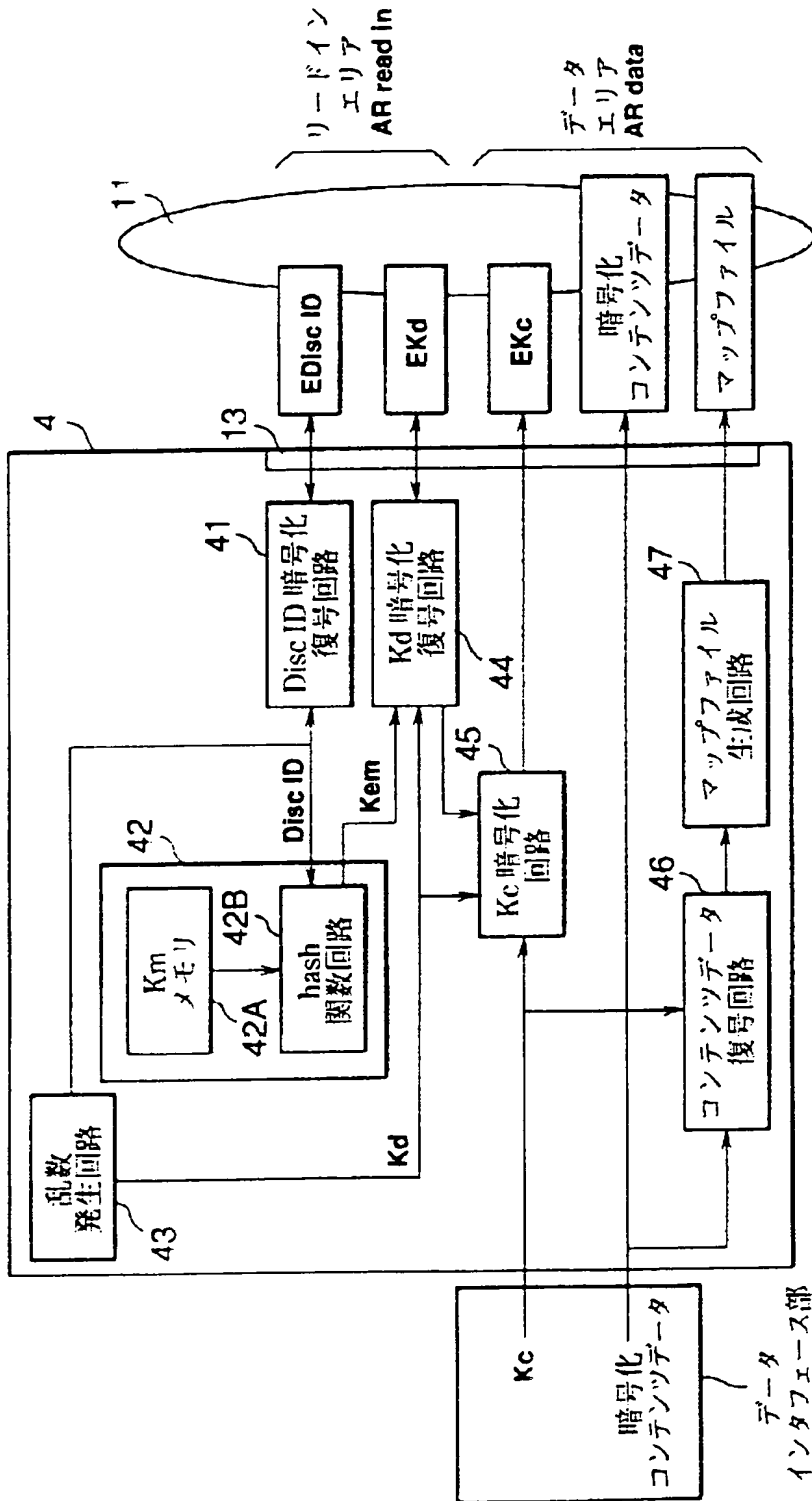
【図 1】



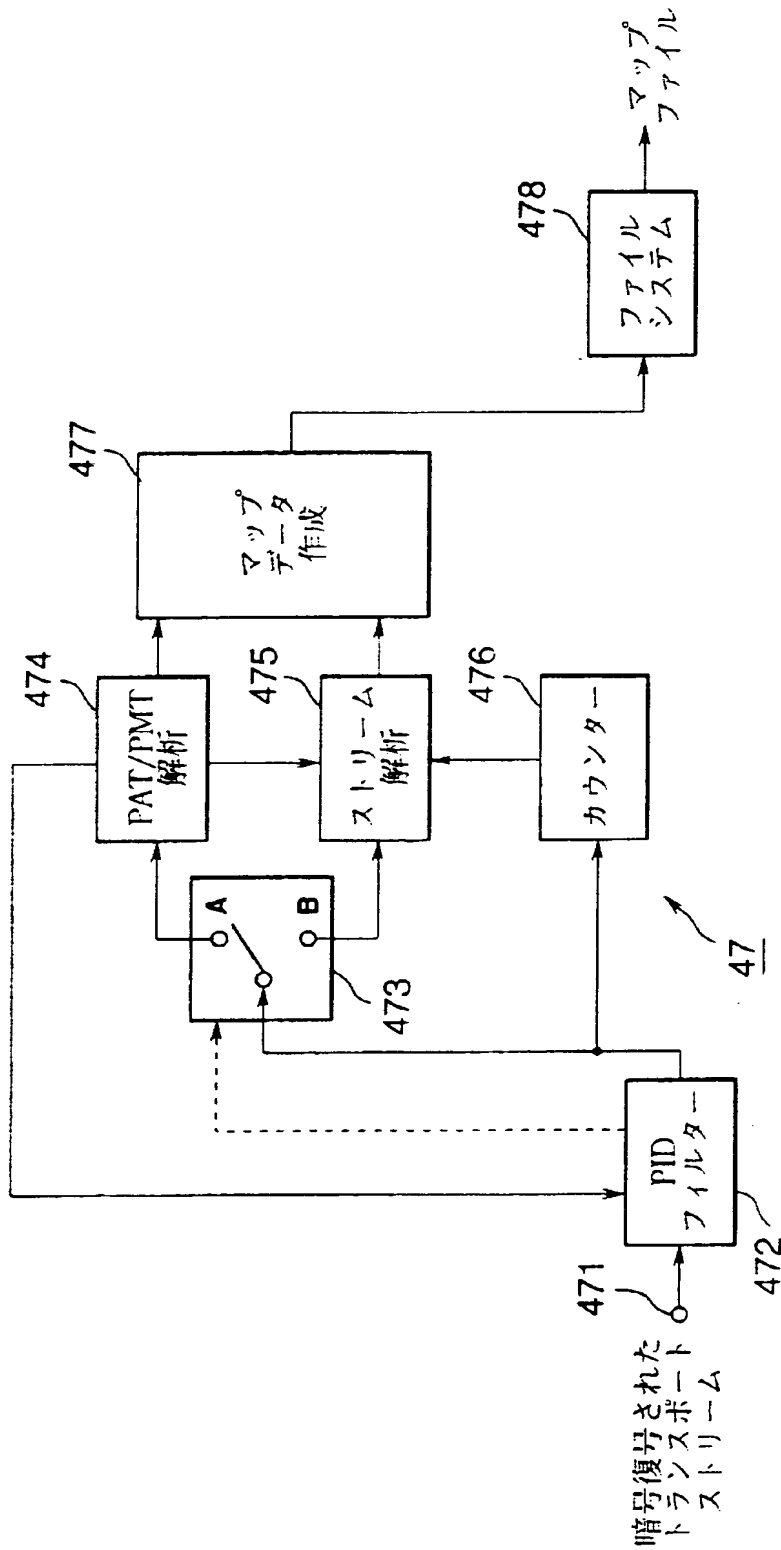
【図 2】



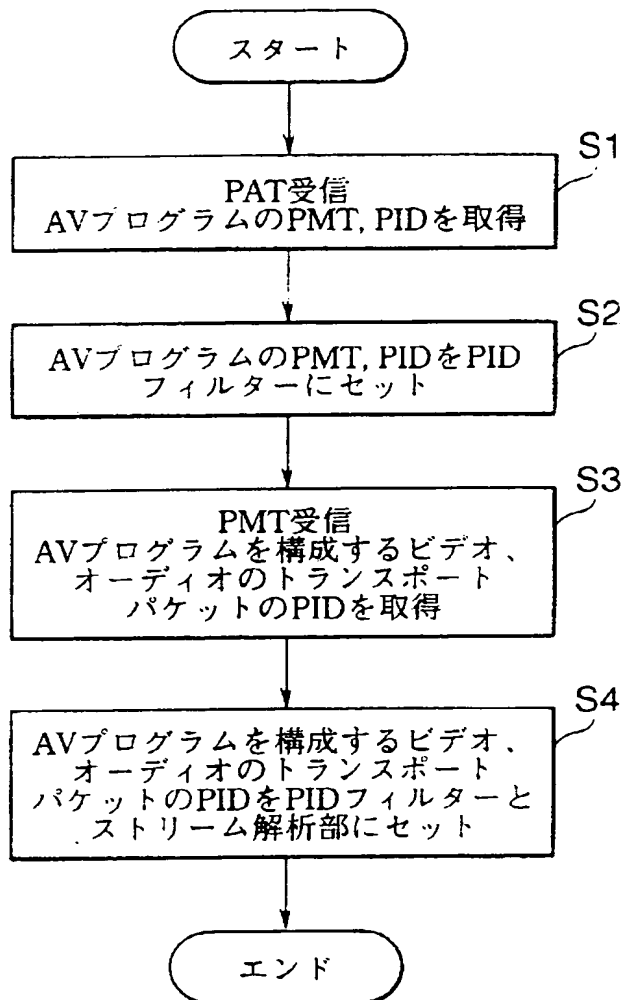
【図 3】



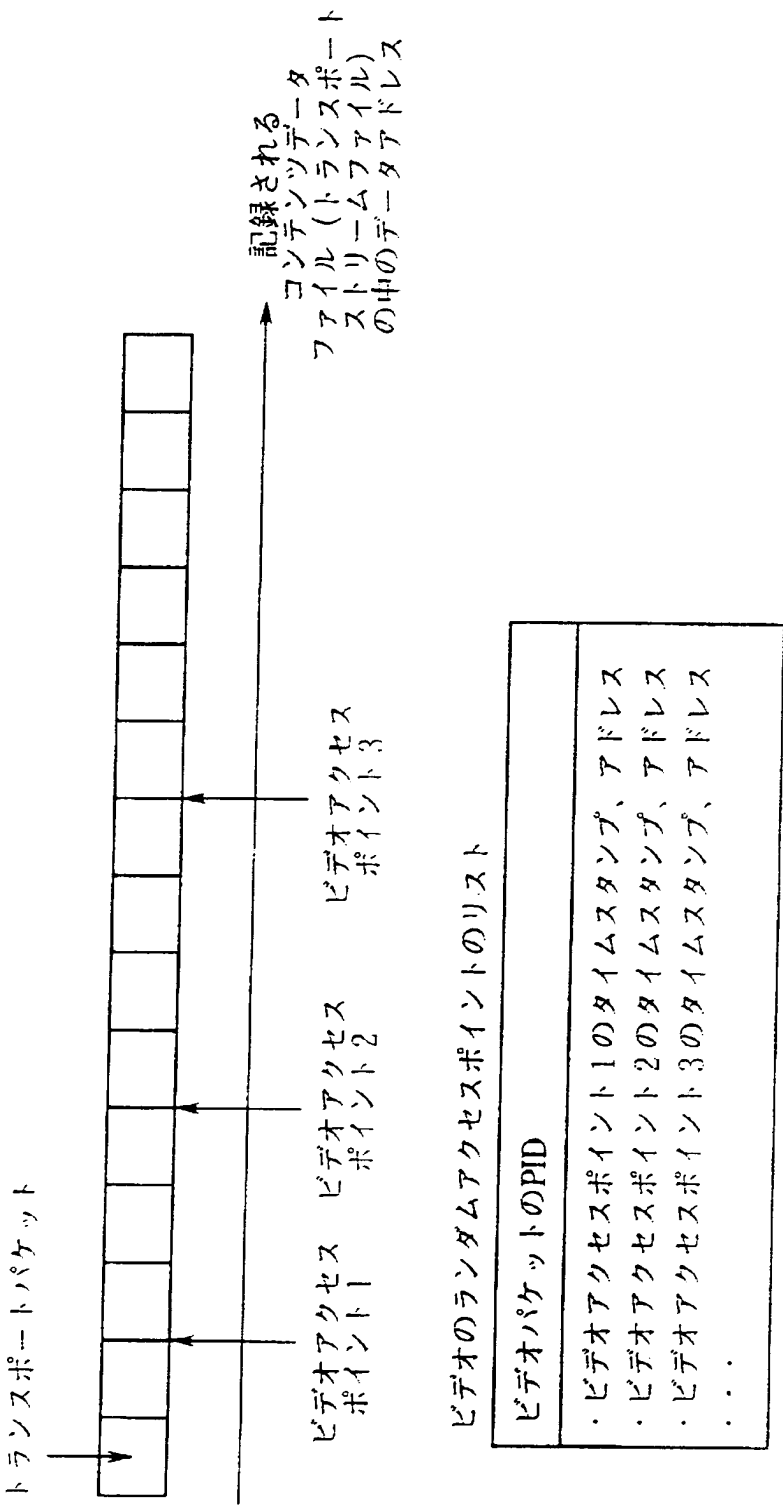
【図 4】



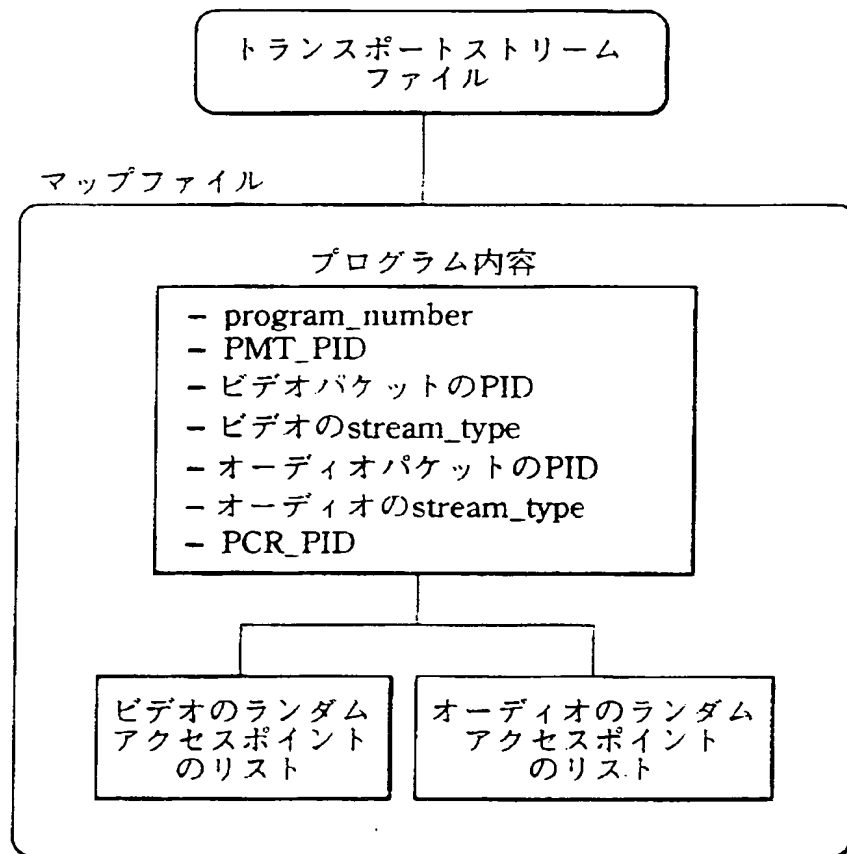
【図 5】



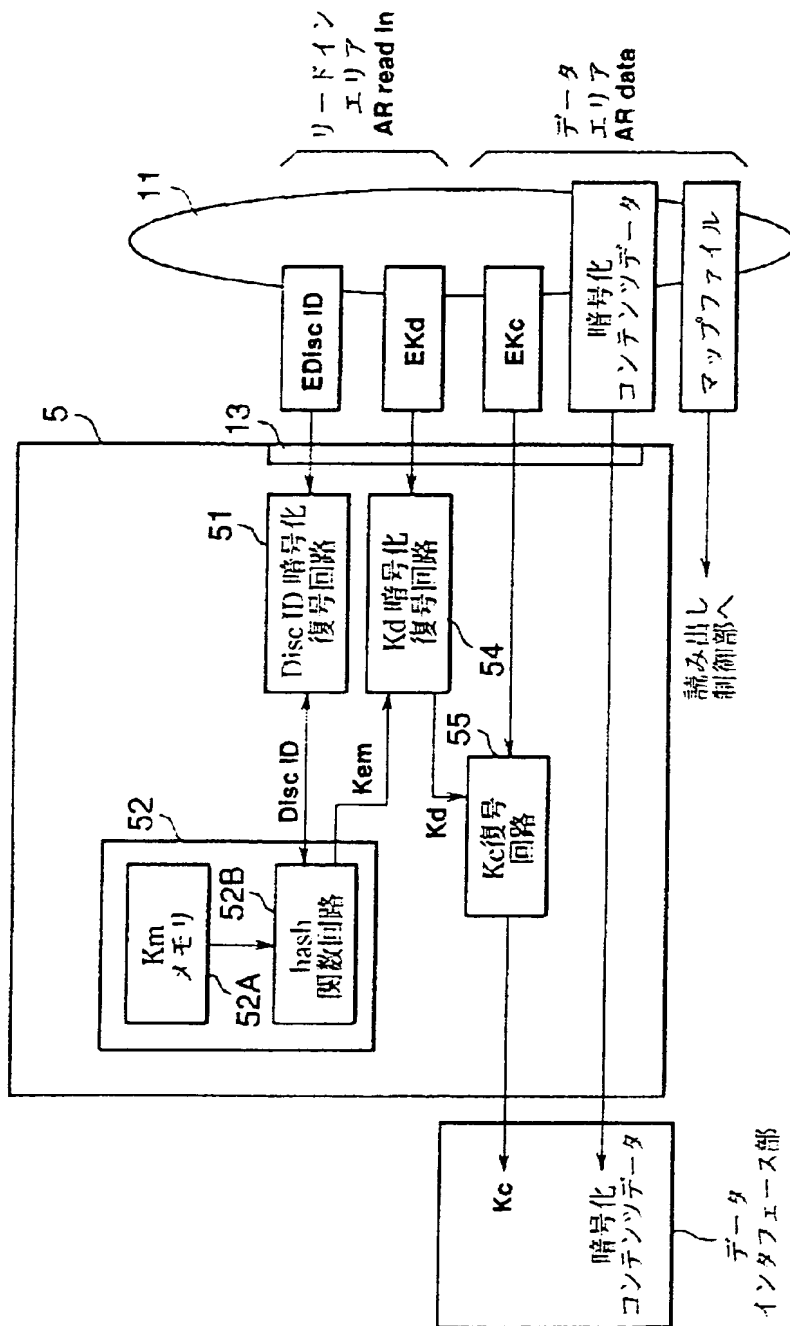
【図 6】



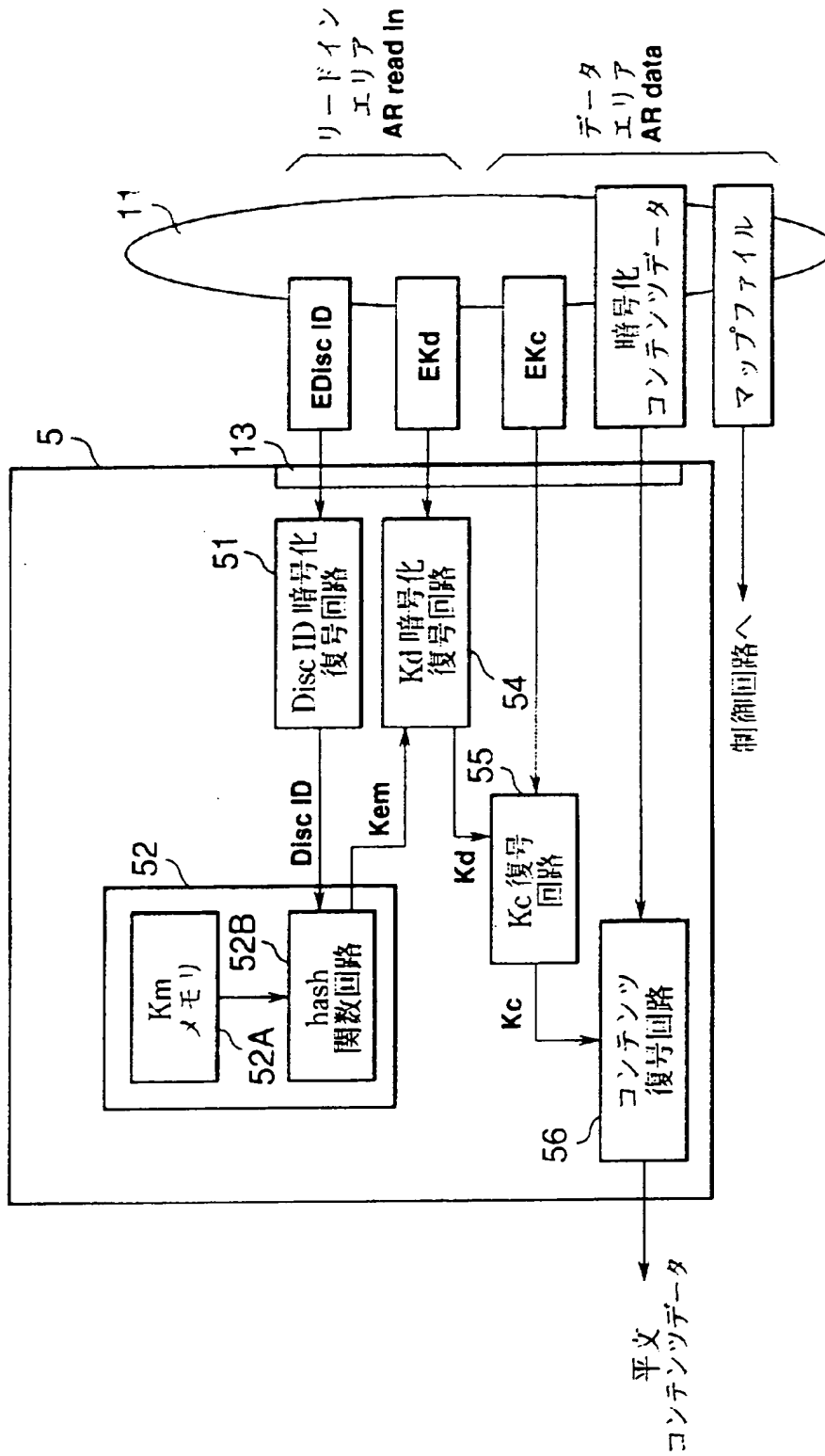
【図 7】



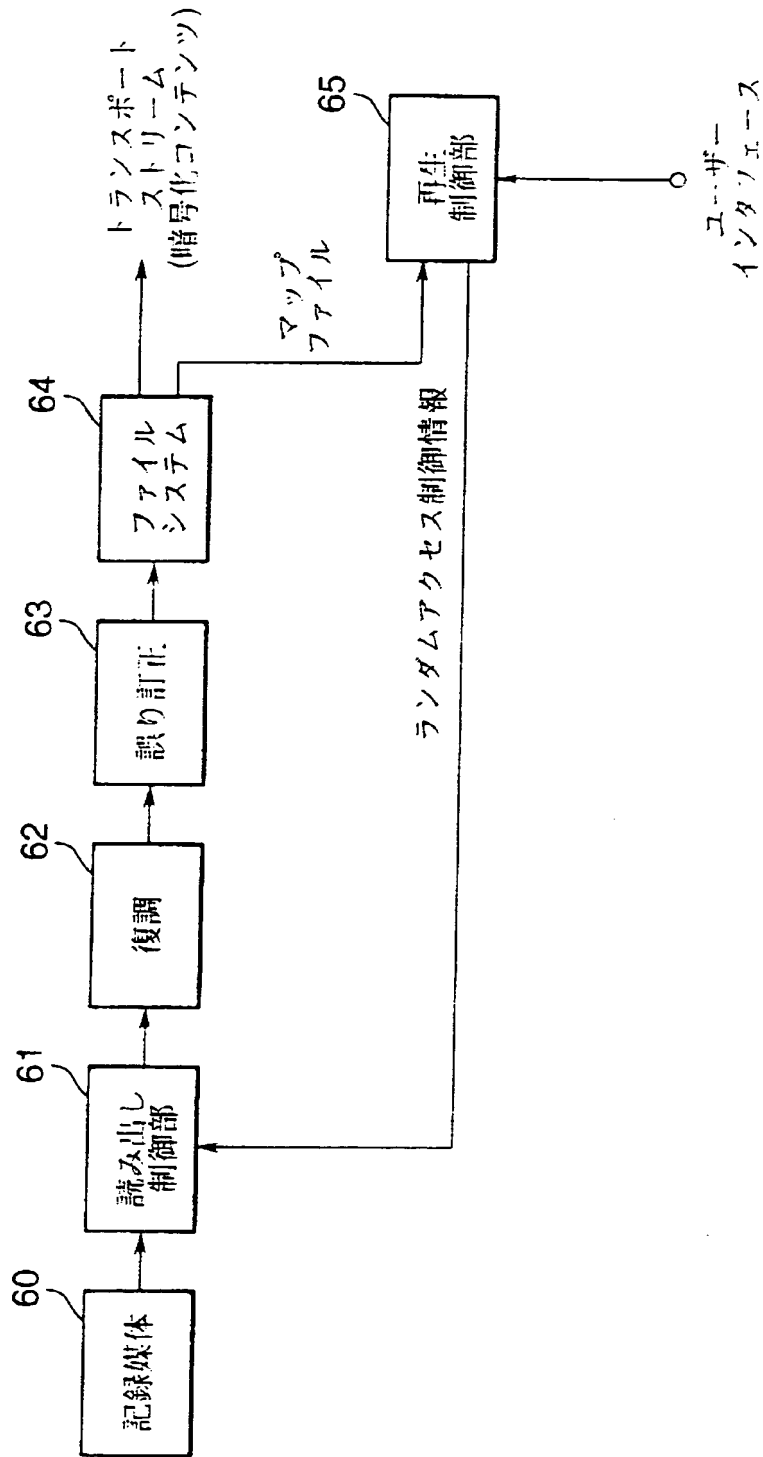
【图 8】



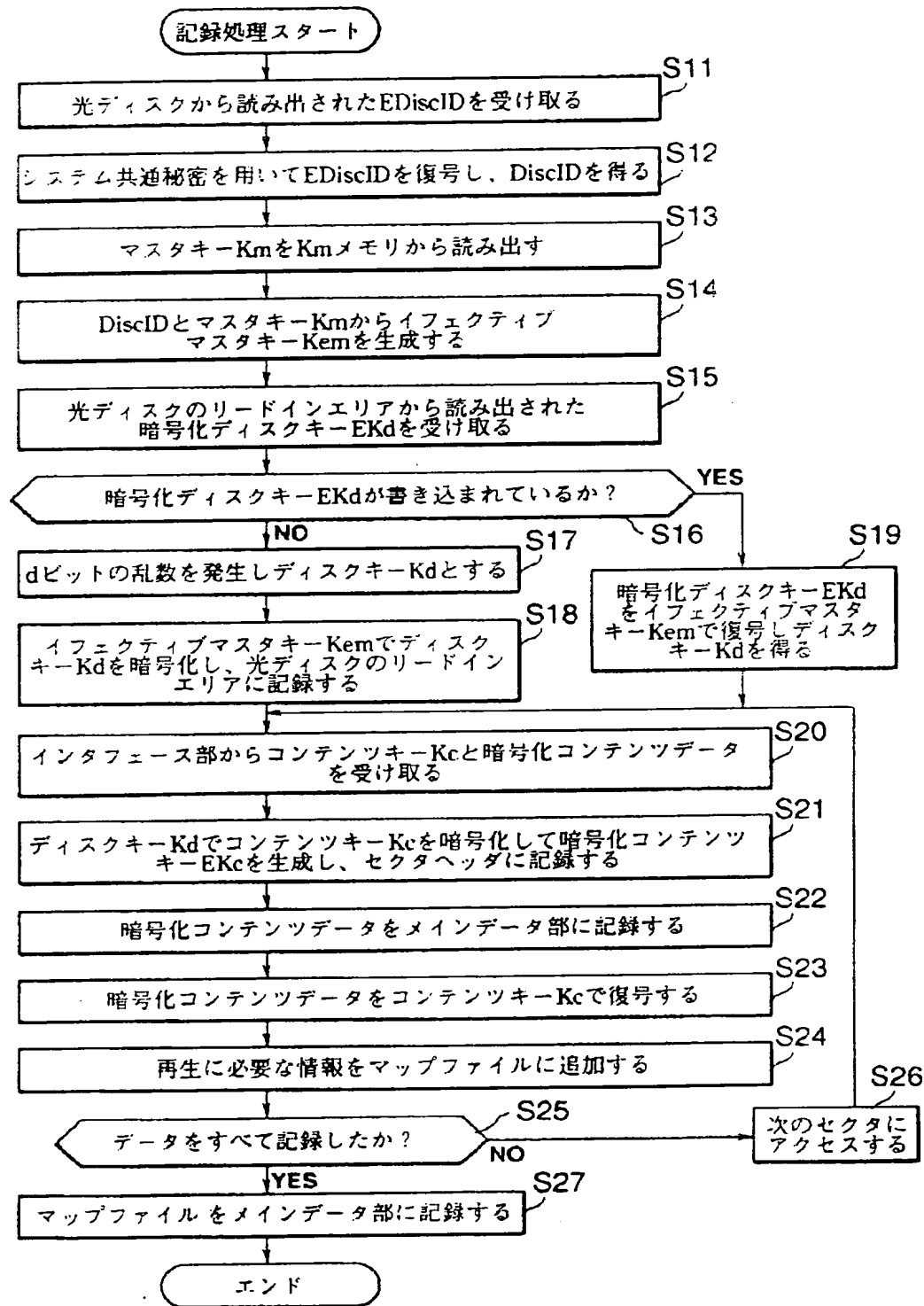
【図 9】



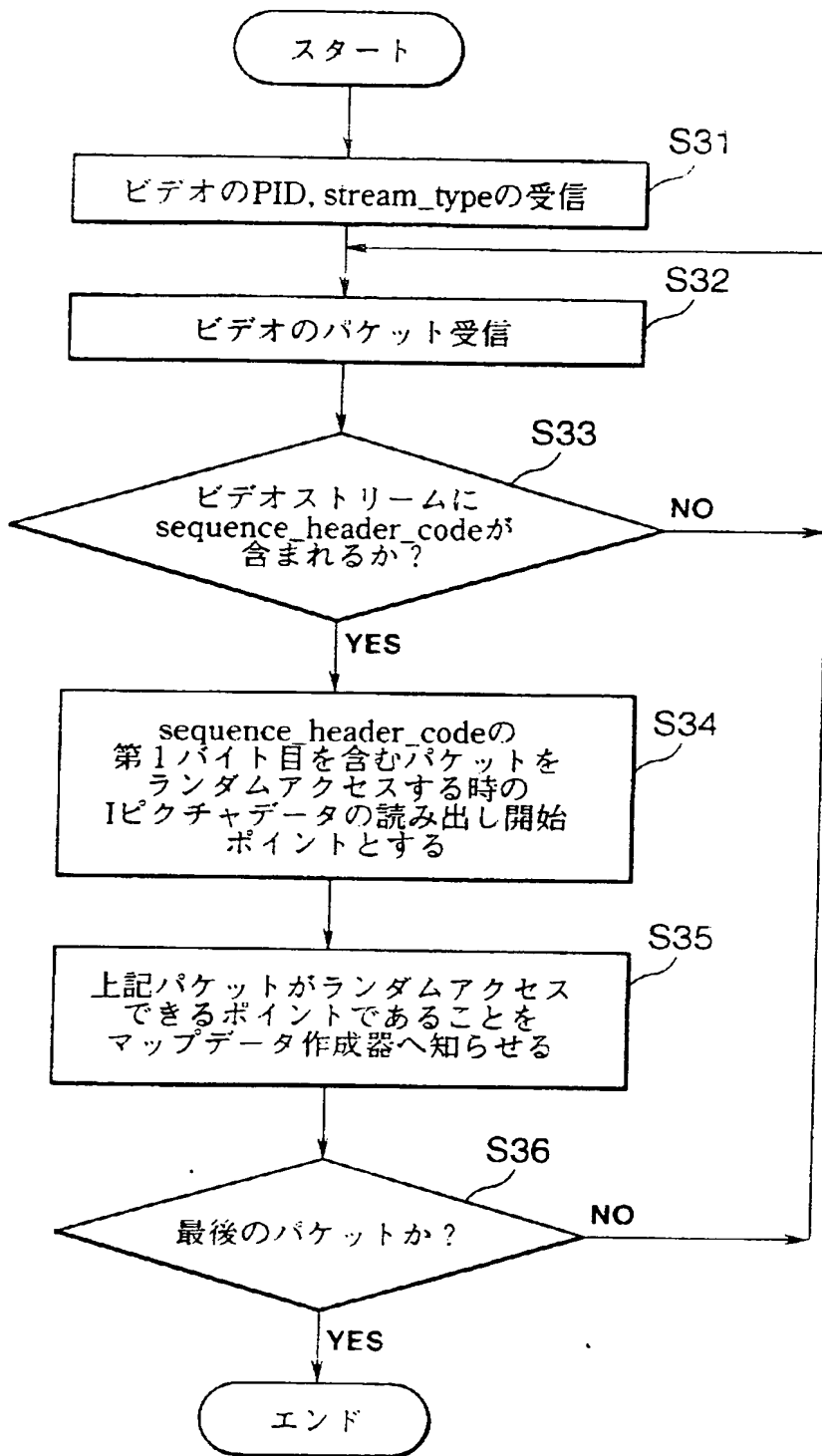
【図 1 0】



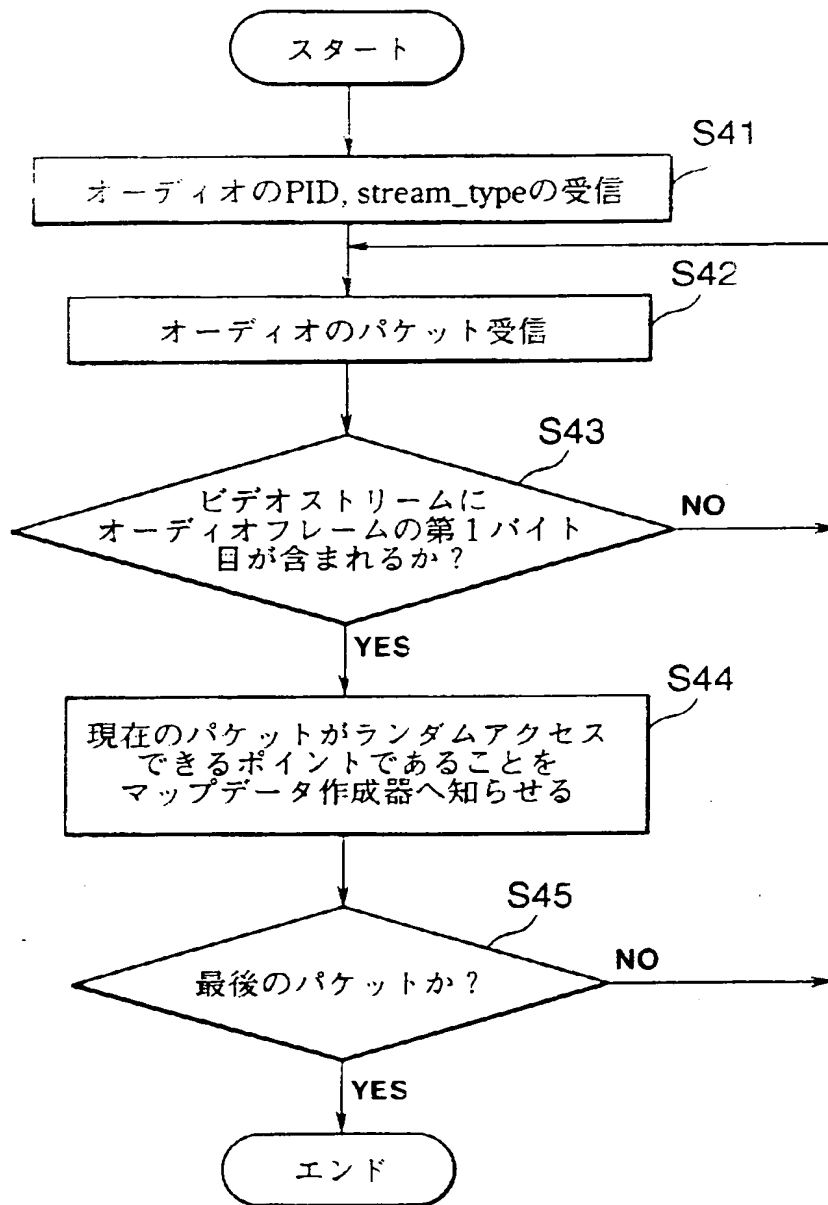
【図 1 1】



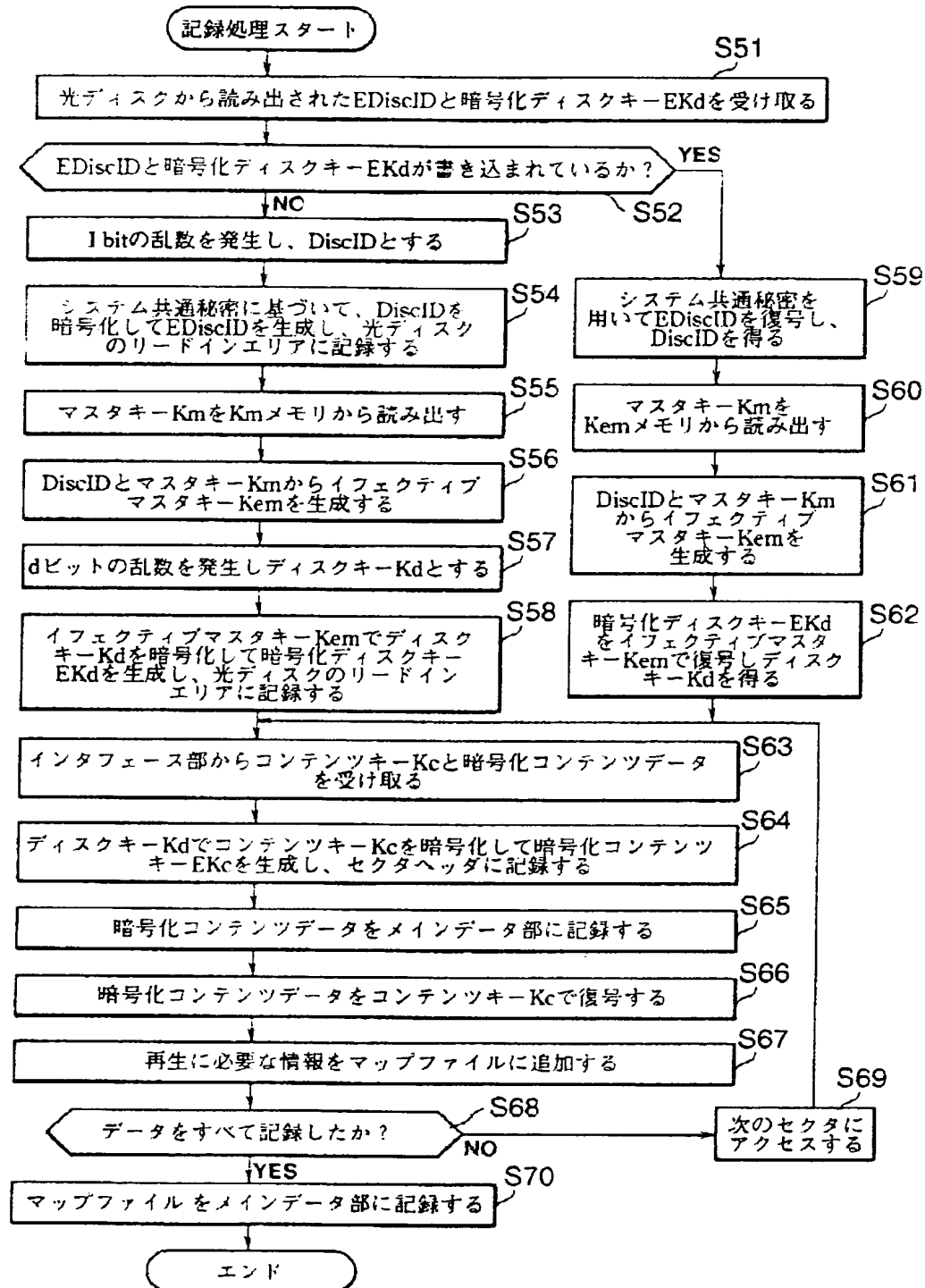
【図 1 2】



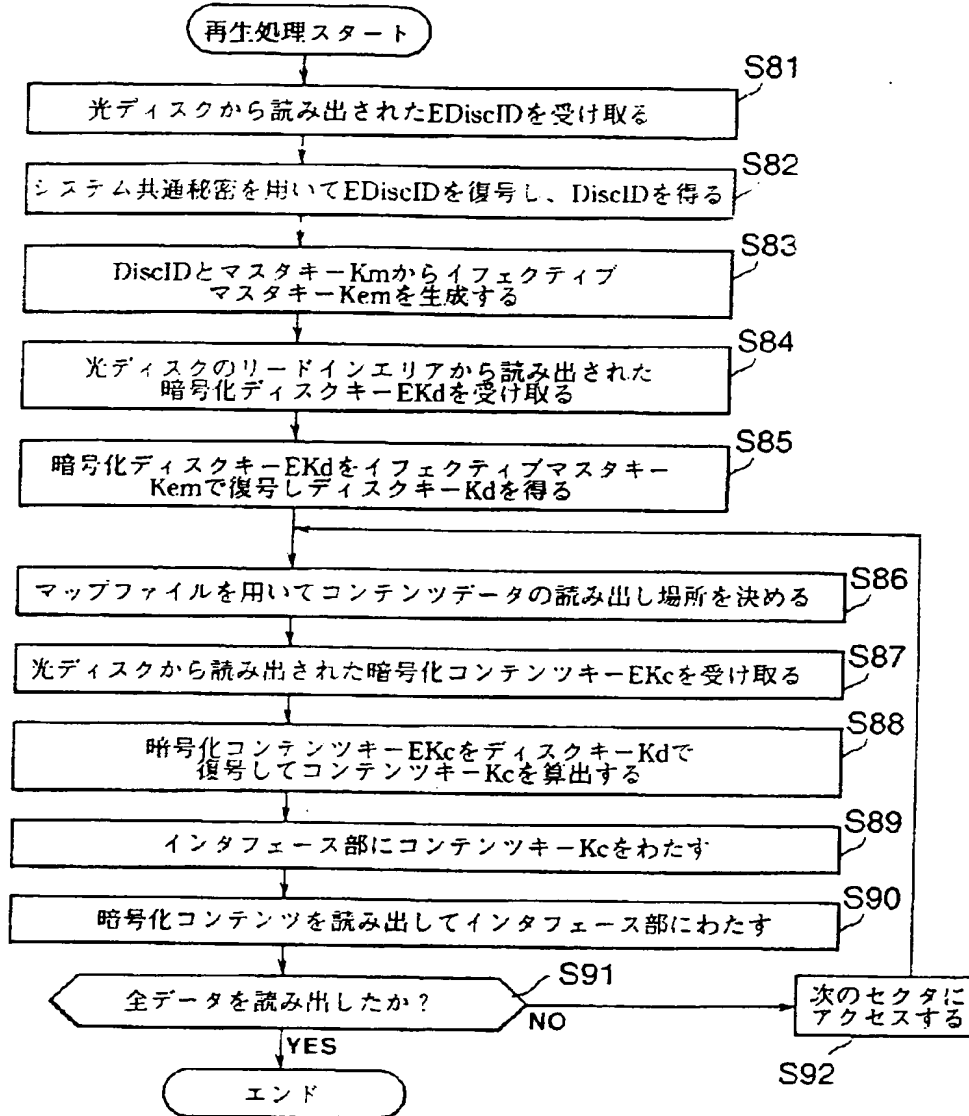
【図 1 3】



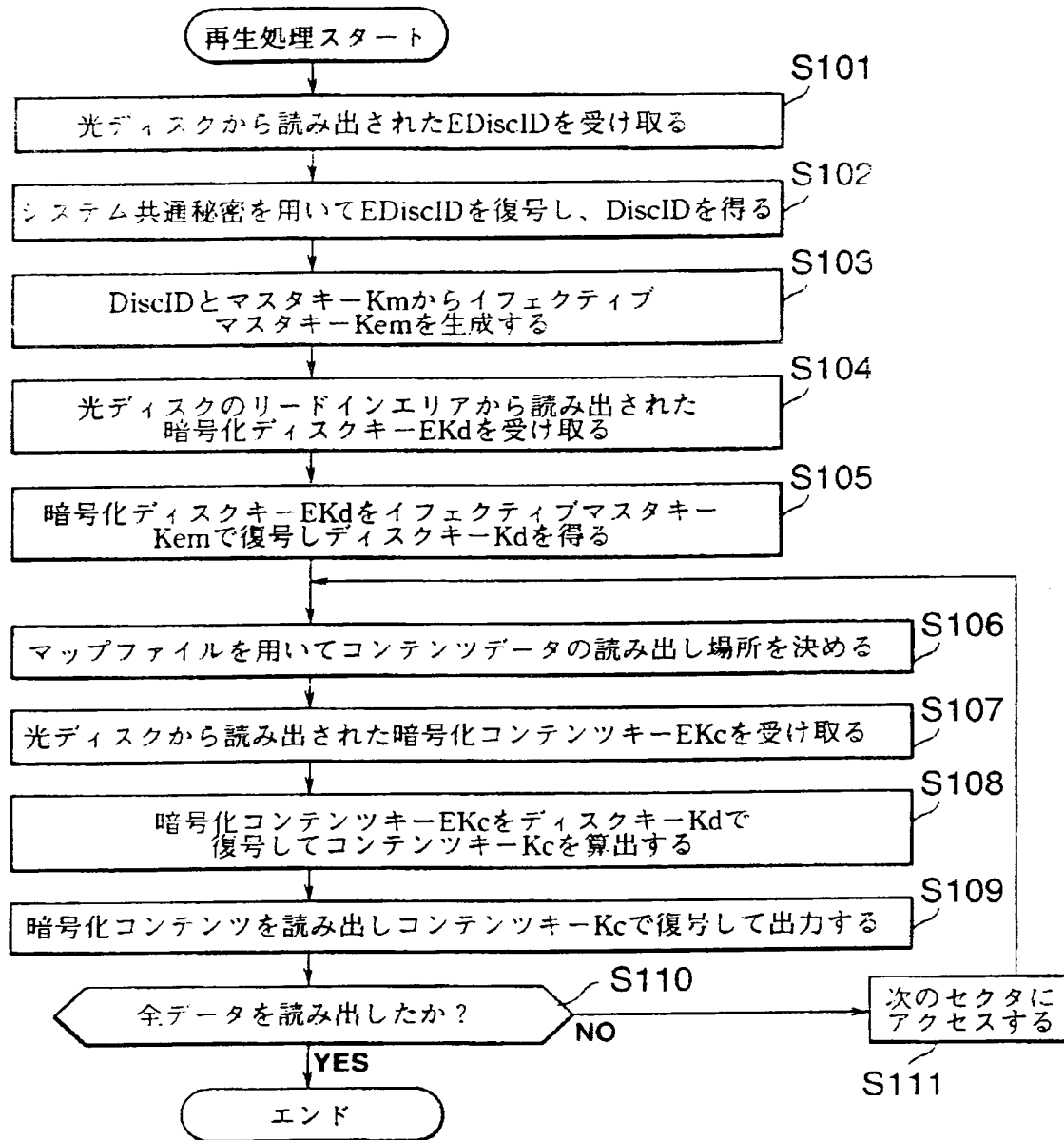
【図 14】



【図 1 5】



【図 1 6】



【書類名】 要約書

【要約】

【課題】 暗号化されて伝送されたコンテンツデータをそのまま記録媒体に記録し、さらにこのデータの暗号化に使用されたコンテンツキーをこの記録システムにおいて用いられる方法で暗号化して媒体に記録し、しかも、きめ細かなトリックプレイを行うことができるようにする。

【解決手段】

記録機器が暗号化されて伝送されたコンテンツデータを記録する際に、コンテンツデータ自体は暗号化されたまま記録媒体に記録するが、コンテンツデータ復号回路 4 6 によりコンテンツデータを復号して、再生時に必要な管理情報を集めたマップファイルをマップファイル生成回路 4 7 を作成し、これをコンテンツデータとともに記録する。

【選択図】 図 3

出 願 人 履 歴 情 報

識別番号 [000002185]

1. 変更年月日	1990年 8月30日
[変更理由]	新規登録
住 所	東京都品川区北品川6丁目7番35号
氏 名	ソニー株式会社